MAANPUOLUSTUSKORKEAKOULU

KOGNITIIVISET TIETOLIIKENNEVERKOT VERKOSTOPUOLUSTUKSESSA

Tutkielma

Kapteeni
Anssi Kärkkäinen

Esiupseerikurssi 63
Maasotalinja

Huhtikuu 2011

MAANPUOLUSTUSKORKEAKOULU

Kurssi	Linja
Esiupseerikurssi 63	Maasotalinja
Tekijä Kapteeni Anssi Kärkkäinen	
Tutkielman nimi **Kognitiiviset tietoliikenneverkot verkostopuolustuksessa**	
Oppiaine, johon työ liittyy Sotatekniikka	Säilytyspaikka Kurssikirjasto (MPKK:n kirjasto)
Aika Huhtikuu 2011	Tekstisivuja 50 Liitesivuja 3

TIIVISTELMÄ

Verkostokeskeinen sodankäynti (*engl. Network Centric Warfare, NCW*) on informaatioylivoiman mahdollistava toimintakonsepti, jonka keskeisin ajatus on kasvattaa sotilaallisen joukon taisteluvoimaa verkottamalla taistelukentän toimijat prosessien, toiminnan ja informaation jakamisen näkökulmasta. Suomessa sodankäyntitavasta käytetään nimitystä verkostopuolustus. Doktriini verkostopuolustuksesta puuttuu, mutta käsite tarkoittaa kaikkien kokonaismaanpuolustuksen toimijoiden verkottamista sosiaalisesti ja toiminnallisesti yhteisten prosessien ja integroitujen tietoverkkojen kautta. Verkostokeskeinen sodankäynti on ensisijaisesti toimintatapamalli, mutta tietoliikenneverkoilla on merkittävä osuus verkostotoiminnan mahdollistajana. Tietoliikennejärjestelmien kehittämisessä on edetty merkittävästi, mutta varsinkin taktisen tason langattomien tietoliikennejärjestelmien rakentaminen on ollut haasteellista.

Verkostopuolustuksen näkökulmasta mielenkiintoinen tutkimusalue on kognitiiviset verkot. Kognitiivinen tietoliikenneverkko on älykäs tietoliikennejärjestelmä, joka tiedostaa järjestelmän sisäisen sekä ympäristön tilan, tekee päätöksen verkon mukauttamisesta annetun tavoitteen saavuttamiseksi ja sen jälkeen konfiguroi verkon asetukset uudelleen. Keskeinen tekijä prosessissa on oppiminen eli kyky hyödyntää aiemmin tehtyjä päätöksiä.

Tutkimuksen ensimmäisen osan tarkoituksena on tarkastella kognitiivisia tietoliikenneverkkoja verkostokeskeisen sodankäynnin paradigmassa ja löytää kohtia, joihin kognitiivinen toiminnallisuus tuo lisäarvoa. Tutkimuksen toisessa osassa vertaillaan muutaman verkon ominaisuuden perusteella nykyisen taktisen tietoliikenneverkon ja kognitiivisen verkon suorituskykyä.

Tutkimuksen tulokset osoittavat, että kognitiivinen verkko tukee verkostopuolustuksen paradigmaa useasta näkökulmasta. Mukautuvalla tietoliikennejärjestelmällä on mahdollista pienentää informaation jakamisen viiveitä ja informaation laatua heikentäviä rajapintoja. Kognitiivinen järjestelmä parantaa taajuuskäytön tehokkuutta ja elektronisen sodankäynnin kykyä.

Kognitiiviset verkot vaativat runsaasti lisätutkimusta mm. tilannetietoisuudesta, päätöksenteosta ja implementoinnista. Taktisella tasolla jatkotutkimusta vaativat kognitiivisen verkon tietoturva ja taistelunkestävyys.

AVAINSANAT

Verkostokeskeinen sodankäynti, verkostopuolustus, kognitiivinen, tietoliikenneverkko

SISÄLLYSLUETTELO

1 JOHDANTO

Yhdysvalloissa 90-lopulla kehitetty verkostokeskeisen sodankäynnin konsepti on levinnyt laajalle varsinkin länsimaisissa asevoimissa. Verkostokeskeinen sodankäynti (*engl. Network Centric Warfare, NCW*) on informaatioylivoiman mahdollistava toimintakonsepti, jonka keskeisin ajatus on kasvattaa sotilaallisen joukon taisteluvoimaa verkottamalla taistelukentän toimijat prosessien, toiminnan ja informaation jakamisen näkökulmasta [4]. Verkottumisen tavoitteena on saavuttaa yhteinen tilannetietoisuus, kasvanut päätöksentekonopeus ja suurempi reagointinopeus, jolloin voidaan tehokkaammin vaikuttaa vastustajaan ja suojata oma toiminta. Verkostokeskeisyys parantaa myös asevoimien itsesynkronointia, millä tarkoitetaan joukkojen kykyä saavuttaa asetettu tavoite ilman ylemmän johdon jatkuvaa ohjausta ja vaikutusta. Perusajatuksena on vähenevien joukkojen ja aselavettien maksimaalinen hyödyntäminen käyttämällä niitä verkottuneesti yhteisoperaatioissa.

Informaatioylivoiman merkittävä tekijä on tehokas tiedon jakaminen verkottuneiden toimijoiden välillä. Avainasemassa on epätietoisuuden hälventäminen taistelukentältä informaatioylivoiman (tiedon jakamisen ja käsittelyn) avulla. Tehokas tietojärjestelmäympäristö erilaisine palveluineen on merkittävä verkostokeskeisen sodankäynnin mahdollistaja, vaikka verkostokeskeisyys ei muodostu pelkästään teknisestä informaationjakamisjärjestelmästä. Verkostopuolustus on ennen kaikkea toiminnallinen ja kulttuurillinen muutos sodankäyntitavoissa [2].

Puolustusvoimissa verkostokeskeinen sodankäynti on määritetty termillä verkostopuolustus, joka kuvaa paremmin toiminnan maanpuolustuksellista luonnetta. Kansainvälisessä toiminnassa käytetään englanninkielistä termiä *Network Enabled Defence* (verkostoavusteinen puolustus). Termi kuvaa hyvin verkon ja verkoston roolia puolustuksen apuvälineenä. Verkostopuolustus on edelleen statukseltaan lähinnä työnimi, vaikka verkostopuolustuksen oppeja sovelletaan kiivaasti. Kansallinen verkostopuolustuksen doktriini tai konsepti puuttuu. Puolustusministeriön tietohallintostrategiassa [39] vuodelta 2007 verkostopuolustus määritellään työnimeksi, jonka perimmäisenä ajatuksena on kuvata strategiselta tasolta aina taisteluteknisselle tasolle ulottuvaa toimintaa, jonka tarkoituksena on mahdollistaa yhteis- ja alueellisten operaatioiden käskytys ja valvonta sekä viranomaisten välinen yhteistoiminta Suomen yhteis-

kunnan elintärkeiden toimintojen turvaamisessa ja kansainvälisessä yhteistoiminnassa. Määritelmä perustuu puolustusvoimain komentajan vuonna 2005 pitämän esitelmään Royal United Services Institute -konferenssissa. Huomattavaa on, että suomalaiseen verkostopuolustuksen käsitteeseen liittyy sotilaallisen verkottumisen lisäksi verkottuminen muihin viranomaisiin sekä kansainvälisiin ja ei-valtiollisiin toimijoihin.

Kuten edellä todetaan, informaation jakaminen ja tehokas tietoliikennejärjestelmä on olennainen osa verkostopuolustusta. Verkostopuolustuksen paradigma asettaa runsaasti vaatimuksia tietoliikennejärjestelmälle verkostoituneessa taistelutilassa. Tietoliikenneverkon on mahdollistettava pääsy tietoon sekä tiedon turvallinen, tehokas ja jatkuva jakaminen toimijoiden välillä. Tietoliikenneteknologia on kehittynyt valtavasti viimeisten vuosikymmenten aikana ja asevoimissakin on runsaasti modernisoitu tietoliikennejärjestelmiä. Merkittävää on ollut kaupallisten teknologioiden kehityksen seuraaminen ja kaupallisten ratkaisujen implementointi sotilaallisiin järjestelmiin. Kehittämisen seurauksena sotilaalliset tietoliikennejärjestelmät ovat monimutkaistuneet, ja sitä myötä niiden käyttö ja hallinta on haastavaa, minkä vuoksi tietoliikennejärjestelmien resurssien käyttö on vain harvoin optimaalista.

Kognitiivisten verkkojen tutkimuksella yritetään ratkaista edellä mainittujen kompleksisten tietoliikenneverkkojen ongelmia. Kognitiivisella verkolla tarkoitetaan yksinkertaisesti älykästä tietoliikennejärjestelmää (muodostuu verkon solmuista sekä langallisista ja langattomista yhteyksistä), joka kykenee tiedostamaan järjestelmän sisäisen sekä ympäristön tilanteen, jonka perusteella järjestelmä toimii adaptiivisesti ja itsenäisesti saavuttaakseen annetun tavoitteen. Tämä edellyttää, että kaikki verkon solmut ja päätelaitteet ovat tilanne- ja kontekstitietoisia. [29]

Kognitiiviset verkot ovat tulevaisuutta, ja niitä tarvitaan yksikertaisesti siitä syystä, että ne mahdollistavat käyttäjien keskittymisen muihin asioihin kuin verkon konfigurointi ja hallinta. Tämän tutkimuksen tarkoituksena on selvittää kognitiivisen verkon tuomaa lisäarvoa verkostopuolustuksen vaatimassa tietoliikenneympäristössä. Työssä perehdytään verkostopuolustuksen paradigmaan ja sitä kautta verkostopuolustuksen asettamiin tiedonjakamisen vaatimuksiin. Näkökulmana on taktinen tietoliikenne, jossa korostuu sotilaallisten tietoliikenneverkkojen kompleksisuus. Taktisella tasolla on paljon eri toimijoita omine järjestelmineen. Yhteistoiminta on rajallista, koska esimerkiksi järjestelmäoperaattoreiden tekemä konfigurointi ja verkonhallinta on haastavaa ja aikaa kuluttavaa.

1.1 Tutkimuksen rakenne, tutkimusongelma ja rajaukset

Tutkimus jakautuu kahteen pääosaan. Ensimmäinen pääosa sisältää paradigmatutkimuksen, jossa tavoitteena on selvittää verkostopuolustuksen tiedon jakamisen problematiikkaa ja vaatimuksia sekä kuvata kognitiivisen verkon konsepti ja perusominaisuudet. Osio tuottaa vaatimukset tietoliikennejärjestelmälle sekä paradigmatason johtopäätökset siitä, miten kognitiivinen tietoliikenneverkko tukee verkostopuolustuksen vaatimuksia. Tutkimusmetodina käytetään kirjallisuusselvitystä.

Toinen pääosa muodostuu taktisen tietoliikenneverkon teknisten suorituskyvyn tarkastelusta. Osiossa luodaan taktiselle tietoliikenneverkolle pelkistetty malli, johon perustuen vertaillaan nykyisen taktisen tietoliikennejärjestelmän ominaisuuksia kognitiivisen toiminnallisuuden sisältävään tietoliikennejärjestelmään. Tietoliikenneverkon monimutkaisuuden vuoksi kaikkien verkon ominaisuuksien vertailu ei ole mahdollista, vaan vertailua tehdään muutaman ominaisuuden suhteen. Ominaisuudet eivät ole pelkästään kognitiivisen järjestelmän ominaisuuksia, vaan yleisiä tietoliikenneverkon ominaisuuksia. Vertailussa joudutaan tekemään yksinkertaistuksia, jotta laskennan monimutkaisuus ei kasva liian suureksi tutkielman laajuus huomioiden. Vertailtavat tekijät on valittu tutkimuksen ensimmäisen osan johtopäätösten perusteella. Vertailun tuloksissa ei pyritä yleistettävään ratkaisuun, vaan esimerkinomaiseen suorituskykytarkasteluun. Osion tutkimusmetodi on matemaattinen analyysi.

Päätutkimuskysymykset ovat:

1. Miten kognitiiviset verkot parantavat tiedon jakamista ja käsittelyä verkostopuolustuksen toimintaympäristössä?
2. Miten kognitiivinen tietoliikennejärjestelmä lisää taktisen tietoliikennejärjestelmään suorituskykyä?

Alatutkimuskysymyksiä ovat:

- Mitä on verkostokeskeinen sodankäynti?
- Miten verkostopuolustus ilmenee taktisella tasolla?
- Mitä vaatimuksia verkostopuolustus asettaa tiedonsiirrolle ja käsittelylle?
- Mitä ominaisuuksia on kognitiivisilla tietoliikenneverkoilla?
- Millainen on taktisen langattoman tietoliikenneverkon perusrakenne?
- Miten verkon suorituskykyä mittaavat ominaisuudet määritetään?
- Mikä on kognitiivisen tietoliikenneverkon suorituskyky eri ominaisuuksien suhteen?

Tietoliikennejärjestelmää tarkastellaan taktisella tasolla, jossa verkko tyypillisesti muodostuu taktisista solmuista ja niiden välisistä langattomista tiedonsiirtoyhteyksistä. Ensimmäisen osan tavoitteena ei ole määritellä täsmällisesti kansainvälinen tai kansallinen verkostopuolustuksen käsite, vaan tavoitteena on johtaa verkostopuolustuksen paradigmasta taktiselle tietoliikennejärjestelmälle vaatimuksia. Vaatimukset voivat olla laadullisia tai määrällisiä. Tutkimuksessa ei tarkastella kognitiivisen verkon implementointimahdollisuuksia eikä järjestelmän kehittämiskustannuksia.

1.2 Tutkimuksen nykytila ja lähdemateriaali

Verkostokeskeisen sodankäynnin tutkimus on jatkunut 1990-lopulta saakka, mutta perusteorian tutkimus on vähentynyt. Tämän hetken tutkimus keskittyy verkostokeskeisen sodankäynnin teorian soveltamiseen käytäntöön erilaisissa sotateknologisissa kehityshankkeissa. Keskeinen tutkimusalue on informaatioteknologia ja sen soveltaminen verkostokeskeiseen toimintaan. Verkostokeskeiseen sodankäynnin paradigman keskeisimmät lähteet ovat 2000-luvun alussa yhdysvaltojen puolustusministeriön alaisessa doktriinitutkimuksessa kirjoitetut teokset *Network Centric Warfare: Developing and Leveraging Information Superiority* [4], *Power to the Edge, Command and Control in the Information Age* [2] ja *Understanding Information Age Warfare* [5].

Edellä mainitut teokset kuvaavat uutta sodankäyntitapaa, jossa informaatioylivoimalla ja verkottumisella luodaan aikaisempaa parempi sotilaallinen vaikutus. Ensimmäinen teos rakentaa verkostokeskeisen sodankäynnin perusteoriaa liikemaailman lainalaisuuksien pohjalta ja toinen teos määrittelee niitä muutoksia, jotka vaaditaan verkostokeskeisen sodankäynnin saavuttamiseen. Teos tarkastelee näitä muutoksia fyysisessä, kognitiivisessa ja informaatioulottuvuudessa. Kolmannessa teoksessa todetaan sotilaallisen ympäristön olevan liian monimutkainen sotilaan tai edes joukon hallittavaksi, jolloin teknologiaa ja verkottumista tarvitaan informaation käsittelyyn ja jakamiseen siten, että ihminen kykenee ymmärtämään kokonaisuutta. Kolmen perusteoksen lisäksi verkostokeskeisen sodankäynnin tarkastelun lähteenä on käytetty yhdysvaltojen kongressin tutkimuspalvelun raporttia [33], jossa kuvataan verkostokeskeisen sodankäynnin taustoja, mutta ennen kaikkea kritisoidaan teorian toimivuutta ja nostetaan esiin doktriinin ongelmia.

Edellä mainitut lähteet kuvaavat verkostopuolustuksen paradigmaa laajasti ja perusteellisesti. Tutkimukset selittävät laajasti verkostokeskeisen sodankäynnin teoriaa, mutta varsinkin ensimmäisten tutkimusten heikkoutena voidaan nähdä vahva teknologiaorientoituneisuus ja verkottumisen keskittyminen vain sotilaallisiin komponentteihin. Toiminnallinen ja sosiaalinen

näkökulma sekä laajempi verkottuminen on tullut yhdysvaltalaiseen tutkimukseen vasta myöhemmin, mutta suomalaisessa käsityksessä kokonaismaanpuolustus ja verkostokeskeisen toiminnan sosiaalinen näkökulma ovat olleet mukana alusta asti.

Kansallisen verkostopuolustuksen paradigman kuvaamiseen on käytetty lähteinä *Verkostoavusteinen puolustus 2030* -kokoelmateosta [42], jossa tarkastellaan verkostopuolustuksen tavoitetilaa useasta eri näkökulmasta tutkimusraporttien kautta. *Näkemyksiä maasodan kuvasta* -kirja [40] kuvaa maasodankäynnin kehittymistä vuoteen 2030 saakka. Verkostopuolustus huomioidaan tässä kehityksessä ja teos pyrkii kuvaamaan sen ilmentymistä maasodankäynnissä. Verkostopuolustuksesta on kirjoitettu myös useissa lehtiartikkeleissa, joista lähteenä on käytetty mm. Kylkirauta-lehden artikkelia *Verkostopuolustus ja taktiset periaatteet: Mikä muuttuu?* [7]. Puolustusministeriön hallinnonalan viralliset asiakirjat määrittelevät verkostopuolustuksen doktriinia niukasti. Ainoa määritelmä virallisista asiakirjoista löytyy puolustusministeriön tietohallintostrategiasta vuodelta 2007 [39]. *Kenttäohjesääntö Yleinen osa* [24] määrittelee puolustusjärjestelmän doktriinin ja mainitsee verkostoituneen puolustuskyvyn, mutta verkostopuolustuksen doktriinia se ei kuvaa edes määritelmätasolla. Suomalaisen lähdeaineiston keskeisin heikkous on verkostopuolustuksen perusteoriaa kuvaavan tutkimuksen puuttuminen.

Kognitiivisia verkkoja tutkitaan nykyään laajasti sekä kotimaassa että ulkomailla, joten aihealuetta käsitteleviä tutkimuspapereita löytyy runsaasti. Aihealueen keskeisimmät lähteet ovat kirjat *Cognitive Networks: Towards Self-Aware Networks* [29] ja *Cognitive radio communications and networks: principles and practice* [53], jotka tarkastelevat analyyttisesti kognitiivisten verkkojen ominaisuuksia teknisestä näkökulmasta. Jälkimmäinen keskittyy kognitiivisiin radioverkkoihin, joissa keskeinen tekijä on taajuuksien älykäs ja tehokas käyttö. Näiden lisäksi lähteinä on käytetty useita tutkimusjulkaisuja [10, 47, 48, 49]. Runsaasta perustutkimuksesta huolimatta kattavaa tutkimusta kognitiivisista verkoista verkostopuolustuksen kontekstissa ei ole laajemmin tehty tai ainakaan julkaistu.

2 KOGNITIIVISET VERKOT VERKOSTOKESKEISEN SODANKÄYNNIN PARADIGMASSA

Termi "verkostokeskeinen sodankäynti" ja niihin liittyviä käsitteitä esiteltiin ensimmäisen kerran vuonna 1990 yhdysvaltain puolustusministeriön laivasto-osaston julkaisussa *Copernicus: C4ISR for the 21st Century* [12]. Ajatuksena oli madaltaa johtamisen hierarkiaa, vähentää operatiivisia taukoja sekä parantaa vaikuttamisen tarkkuutta ja käskytysnopeutta verkottamalla sensorit, komentajat ja tulenkäyttö. Kognitiivinen verkko on uudempi käsite [47] ja sillä pyritään kuvaamaan tietoliikenneverkon kykyä kognitiiviseen toimintaan. Luvun tarkoituksena on paradigmatasolla tarkastella verkostopuolustusta ja kognitiivisia verkkoja ja tutkia, miten kognitiiviset verkot voisivat parantaa verkostopuolustuksen tietoliikennejärjestelmien suorituskykyä.

2.1 Verkostokeskeisen sodankäynnin paradigma

Yhtenäisenä konseptina verkostokeskeinen sodankäynti kuvattiin vuonna 1998 US Naval Instituutin julkaisussa ja syvemmin samana vuonna ilmestyneessä J. Garstkan, D. S. Albertsin ja F. Steinin kirjassa *Network Centric Warfare* [4]. Verkostokeskeinen sodankäynti on kuvattu informaatioajan (*engl. Information Age*) sodankäynniksi, jonka teoria voidaan kiteyttää neljään dogmiin eli perusoppiin [4]. Nämä ovat:

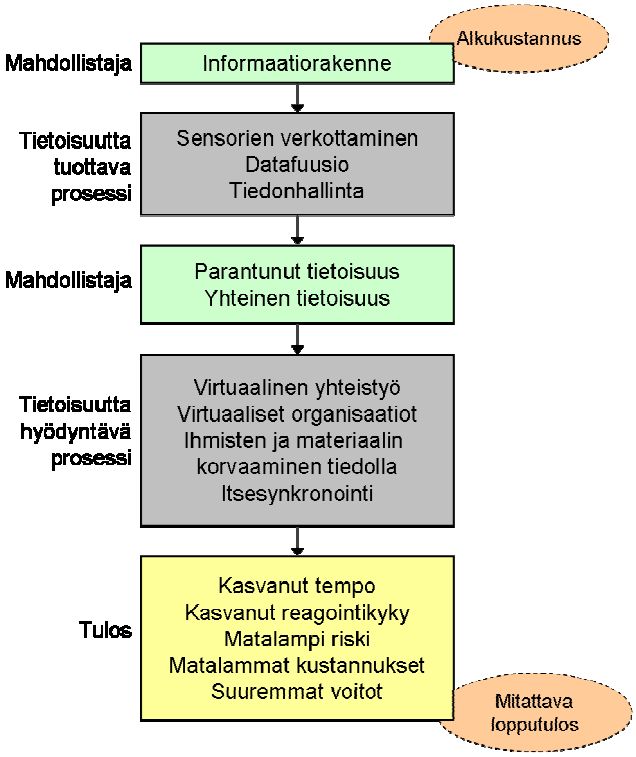
1. Kestävästi ja vahvasti verkottuneet voimat parantavat informaation jakamista.
2. Tiedonvaihto parantaa tiedon laatua ja yhteistä tilannetietoisuutta.
3. Yhteinen tilannetietoisuus mahdollistaa yhteistyön ja itsesynkronoinnin, ja parantaa taistelunkestävyyttä sekä komentonopeutta.
4. Kohdan 3 tekijät (yhteistyö, itsesynkronointi, taistelunkestävyys, komentonopeus) puolestaan kasvattaa dramaattisesti operaation tehokkuutta.

Kuten neljästä perusopista huomataan, informaation jakaminen on operaation onnistumisen kannalta keskeisin tekijä. Ilman tehokasta ja jatkuvaa informaation jakamista muut perusopit (2 - 4) menettävät merkityksensä. Kuvassa 1 on esitetty edellä esitetyistä perusopeista muodostuva arvoketju (*engl. Value Chain*), joka pyrkii kuvaamaan verkostokeskeisen sodankäynnin hyötyjen ja tehokkuuden saavuttamista perusoppien kautta.

Arvoketju alkaa informaatiorakenteesta, joka mahdollistaa prosessit, jotka synnyttävät huomattavasti paremman kilpailuympäristön tilannetietoisuuden ja sen jakamisen koko organisaation läpi. Tämä puolestaan mahdollistaa joukon prosesseja, jotka hyödyntävät tätä tietoisuutta

siten, että lopputulos paranee. Sodankäynnissä nämä tulokset ovat kasvanut taistelunopeus (tempo), pienemmät riskit ja kustannukset (tappiot) ja suurempi vaikuttavuus.

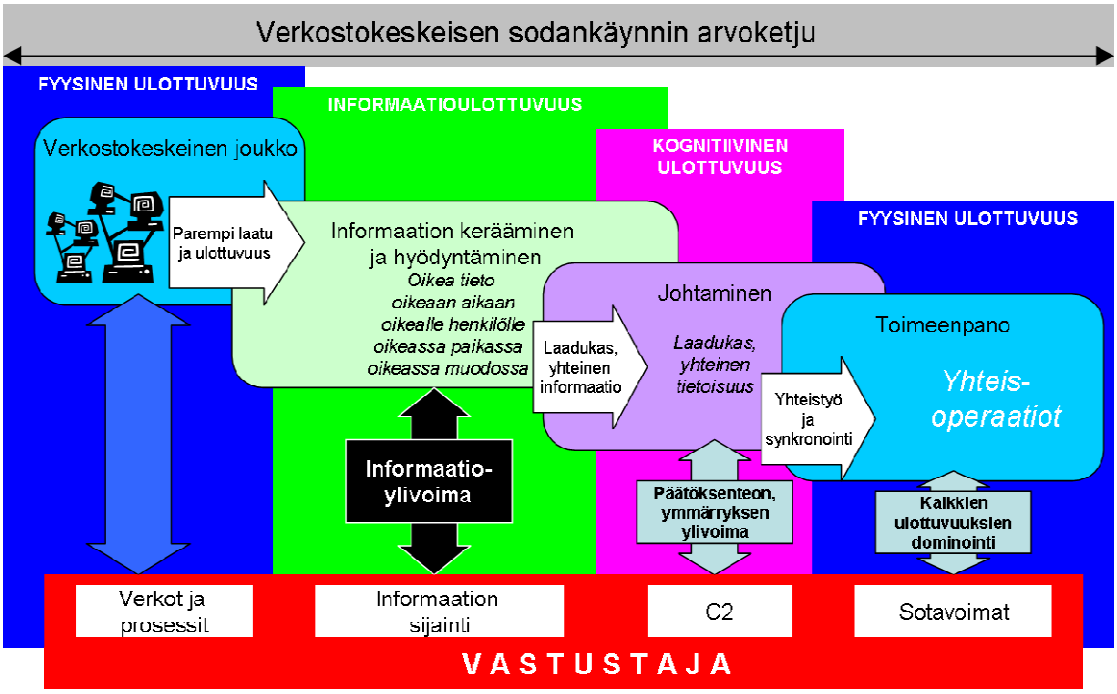
Vuonna 2001 julkaistussa teoksessa *Understanding Information Age Warfare* [5] pyrittiin edelleen kehittämään NCW-konseptia rakentamalla sodankäynnin operatiivista teoriaa. Keskeinen käsite teoksessa on informaatioylivoima. Teoriaa lähdettiin kehittämään tarkastelemalla ympäristön havainnointia kolmessa ulottuvuudessa.



Kuva 1. Verkostokeskeinen organisaation arvoketju.

Fyysisessä ulottuvuudessa ovat ne tapahtumat, jotka voidaan havaita sensorin ja yksilön toimesta. Fyysistä ulottuvuutta ovat maa-, meri-, ilma- ja avaruusympäristöt, joissa sotajoukot suorittavat operaatioita. Fyysisessä ulottuvuudessa sijaitsevat myös joukot yhdistävät viestintäverkot. Fyysisestä ulottuvuudesta syntyvä data kuljetetaan *informaatioulottuvuuden* läpi. Informaatioulottuvuudessa tietoa luodaan, muokataan ja jaetaan. Informaatioulottuvuudessa tapahtuu yksiköiden välinen tiedonvaihto, kommunikointi sekä käskyttäminen. Informaatioulottuvuudessa sijaitsevat sensorit ja niiden tuottama tieto sekä analysoitu tieto. Data vastaanotetaan ja prosessoidaan *kognitiivisessa ulottuvuudessa*, jossa se arvioidaan ja jonka pohjalta käynnistetään toiminta. Kognitiivinen ulottuvuus on taistelijan mieli. Tämän ulottuvuuden elementtejä ovat esimerkiksi johtajuus, moraali, koulutustaso ja kokemus sekä tilannetietoisuus.

Mielenkiintoista on havaita, miten edellä kuvattu prosessi toistaa John Boydin OODA (Observe, Orient, Decide and Act) -silmukan [9] prosessia. Kuvassa 2 on esitetty NCW-teoksessa kuvattu verkostokeskeisen sodankäynnin arvoketju ja sen linkittyminen edellä mainittuihin ulottuvuuksiin.



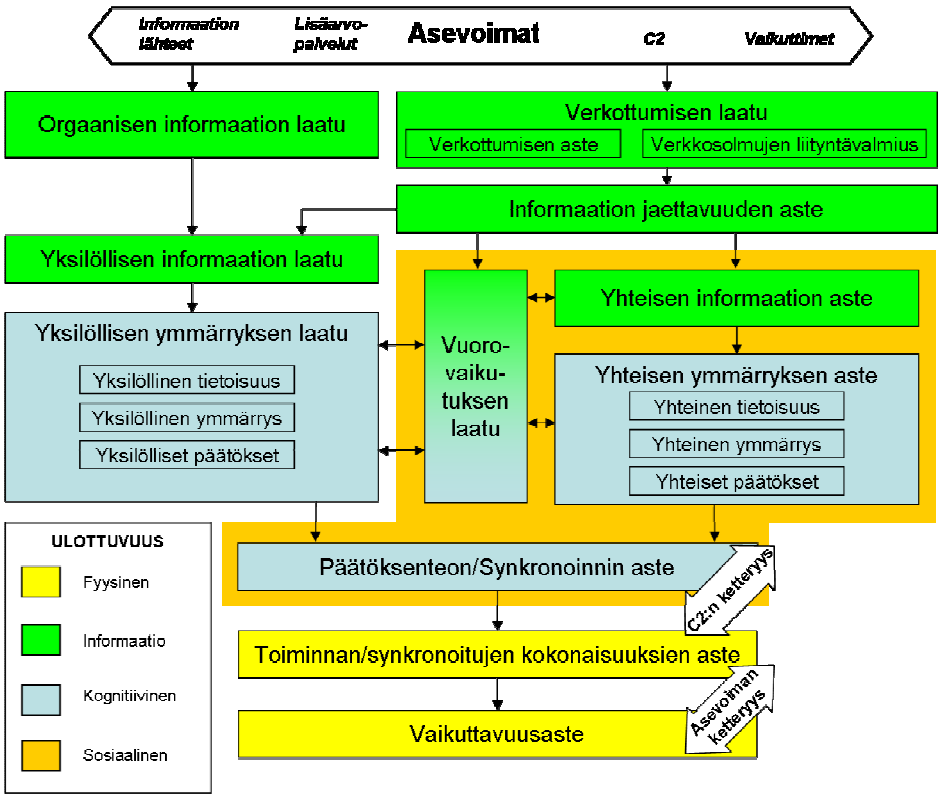
Kuva 2. NCW-arvoketjun linkittyminen informaatioylivoimaan (kolmeen ulottuvuuteen).

Kolmas ja viimeinen NCW-teoriaa kehittävä julkaisu *Power to the Edge* [2] ilmestyi vuonna 2003. Kirja on spekulatiivinen tutkimus, jonka perusolettamus on se, että nykyaikaiset sotilaallisen ympäristöt ovat liian monimutkaisia yksilön, organisaation tai jopa asevoimien ymmärrettäviksi. Nykyaikainen tietotekniikka mahdollistaa nopean ja tehokkaan tietojen jakamisen siten, että ”reunakäyttäjien" tai sotilasoperaatioita toteuttavien tulisi itse hakea informaatiota tietovarannoista sen sijaan, että keskitetyt toimijat yrittävät arvata käyttäjien tietotarpeet ja työntävät informaatiota heille. Haasteeksi todetaan edellä mainitun toiminnan edellyttämä sotilashierarkian madaltaminen. Teoksen visioiden realisoitumisesta ei ole varmuutta, mutta jonkinlaisena ensiaskeleena voidaan pitää Yhdysvaltain globaalin tietoverkon (*engl. Global Information Grid*) toteuttamista [15]. Myös puolustusvoimien integroitu tiedustelun, valvonnan ja johtamisen järjestelmäkokonaisuuden (ITVJ) voidaan todeta perustuvan edellä mainittuun ajatukseen.

Alkuperäistä NCW-paradigmaa on kritisoitu teknologian ihannoinnista ja mallin teknologiakeskeisyydestä. Mallin kehittämisessä edettiin pitkään teknologiapainotteisesti ja uusien teknologioiden ohjaamina. Yhdysvaltain viime vuosien sotakokemukset ovat kuitenkin osoit-

taneet nykyteknologian rajoitteet verkostokeskeisen sodankäynnin toteuttamisessa. Suuri määrä informaatiota ja ylivertaiset tietojärjestelmät eivät automaattisesti tarkoittaneet informaatioylivoimaa. Verkostokeskeinen sodankäynti onkin opillisesti edennyt vajaan kahden vuosikymmenen aikana teknologiapainotteisesta opista hyvin vahvasti johtamista sekä vaikutuksia painottavaksi ajattelumalliksi. Se pyrkii nostamaan esiin informaatioajan mahdollisuuksia, joita teknologian hyödyntäminen edesauttaa. Terminologisesti verkostokeskeinen sodankäynti on jo jokseenkin vanhentunut. Tilalle ovat tulleet termit verkostokeskeiset operaatiot (*engl. Network Centric Operations, NCO*) [8] sekä vaikutuspohjaiset operaatiot (*engl. Effect Based Operations EBO, ja Effect Based Approach to Operations, EBAO*) [11]. Tosin eräät tahot ovat jo ilmaisseet, että terminä EBO on pohjimmiltaan epäkelpo [30]. Termistä on liian monta tulkintaa, ja käsite on ristiriidassa sodan luonteen kanssa lisäten epäjärjestystä taistelukentällä. EBO edellyttää sodankäynnin ennustettavuuden olevan tasolla, jota ei käytännössä voida saavuttaa.

Verkostokeskeiset operaatiot -käsitteellä pyritään kuvaamaan laajemmin verkostokeskeisyyttä, eikä se rajoitu pelkästään sodankäyntiin, vaikkakin sotilaskontekstissa termi kuvaa ennen kaikkea uutta sodankäyntitapaa [18]. Verkostosodankäynnin dogmeille kehitettiin metriikkaa, minkä tuloksena syntyi verkostokeskeisten operaatioiden käsitekehikko (*engl. NCO Conceptual Framework*). Kehikon ylin taso on esitetty kuvassa 3.



Kuva 3. NCO-käsitekehikko [18].

Kehikko on yleistetty prosessimalli, jossa tunnistetaan sosiaalisen ulottuvuuden rooli, ajattelun tärkeys ja joka identifioi avainkonseptit ja potentiaaliset riippuvuudet. Kehikko muodostuu käsitteistä (konsepteista), joille on määritetty alemman tason ominaisuudet ja metriikka. Kehikko on skaalautuva, ja sen idea on tuottaa perusrakenne NCW-hypoteesien kvantitatiiviselle mittaamiselle.

Kehikosta voidaan havaita, miten teoria olettaa informaation ja verkottumisen laadun parantavan yksilöllisen ja yhteisen ymmärryksen laatua, ja sitä kautta päätöksentekoa ja synkronoinnin astetta. Lopputuloksena on laadukkaampi toiminta ja paremmin synkronoidut kokonaisuudet (asevoimien osat), mikä johtaa lopulta parempaan vaikuttavuuteen. Kuvasta 2 nähdään myös, missä osissa kehikkoa eri ulottuvuudet vaikuttavat. Huomattavaa on, että aiemmin mainittujen ulottuvuuksien (fyysinen, informaatio ja kognitiivinen) lisäksi kehikko sisältää sosiaalisen ulottuvuuden, jonka merkitystä ei voi aliarvioida. Sosiaalisessa ulottuvuudessa tapahtuu kaikki ihmisten välinen yhteistoiminta. Tässä ulottuvuudessa ihmiset ovat vuorovaikutuksessa keskenään, vaihtavat tietoa, muodostavat yhteistä tilannetietoisuutta ja tekevät yhteisiä päätöksiä. Sosiaalisessa ulottuvuudessa vaikuttavat myös elementit kuten kulttuuri, arvot ja asenteet.

Jokainen ylimmän tason käsite kuvataan joukkona ominaisuuksia (atribuutteja) ja metriikkoja alemmalla tasolla. Attribuutit kuvaavat käsitteen ominaisuuksia laadullisesti ja määrällisesti. Kukin attribuutti on todellisuudessa mitattu metriikalla (tai metriikoilla), joka määrittelee yksityiskohtaisesti, mitä tietoja olisi tarpeen kerätä attribuuttia arvioitaessa. Tietoliikenteen kannalta merkittävä ominaisuus on verkottumisen laatu, joka muodostuu liityntävalmiista verkkosolmuista ja verkottumisen asteesta. Verkottumisen asteen attribuutteja ovat saavutettavuus, palvelun laatu sekä tiedon turvaaminen. Esimerkiksi saavutettavuuden metriikkana voi olla niiden verkonsolmujen osuus, jotka voivat kommunikoida halutulla tavalla eli ovat saavutettavissa. Liityntävalmiin verkkosolmun tärkein ominaisuus on kyky kommunikoida verkon muiden solmujen kanssa halutulla tavalla. [18]

Vaikka tässä yhteydessä NCW-paradigman kuvaamisessa on tyydytty tarkastelemaan yhdysvaltalaista kehitystä, verkostokeskeisen sodankäynnin paradigma on osa sodankäynnin kehittämistä useissa maissa ympäri maailmaa. Paradigman tarkastelu yhdysvaltalaisesta näkökulmasta on perusteltua, koska NCW-konsepti kehitettiin alun perin Yhdysvalloissa. Lisäksi yhdysvaltalaista tutkimusta on julkaistu avoimesti, ja Yhdysvalloilla on ollut resursseja kehittää konseptia edelleen. Huomioitavaa on myös se, että muiden maiden tutkimus perustuu juuri

yhdysvaltalaiseen perustutkimukseen. Esimerkkeinä muiden maiden tutkimuksesta ja näkökulmista voidaan mainita Iso-Britannian, Ruotsin ja Naton verkostokeskeisyyttä määrittelevät konseptit [21, 35, 50].

Verkostokeskeisyyden paradigmaa tarkastellessa voidaan huomata, että jo pari vuosikymmentä vanhat perusopit eivät ole muuttuneet, vaikka uusia käsitteitä ja toimijoita on tullut lisää. Edelleenkin ylivoimaa pyritään hankkimaan tilannetietoisuudella, tehokkaalla tiedon jakamisella ja käsittelyllä. Sosiaalisen ja humaanin toiminnan rooli on korostunut, mutta edelleen nähdään, että tietojärjestelmät ja tietoliikennejärjestelmät ovat avainroolissa toimijoiden välisten verkostojen rakentamisessa.

2.2 Verkostopuolustus suomalaisena käsitteenä

Verkostokeskeistä sodankäyntiä kuvaavana terminä verkostopuolustus (Network Enabled Defence, NED) on ollut puolustusvoimissa vakiintuneena käsitteenä jo useita vuosia. Käsitteen käyttöä on kuitenkin hankaloittanut määrittelyn vajavaisuus. Vaikka termiä käytetään yleisesti, sitä ei ole määritetty yksiselitteisesti esimerkiksi puolustusvoimien doktriinitason asiakirjassa.

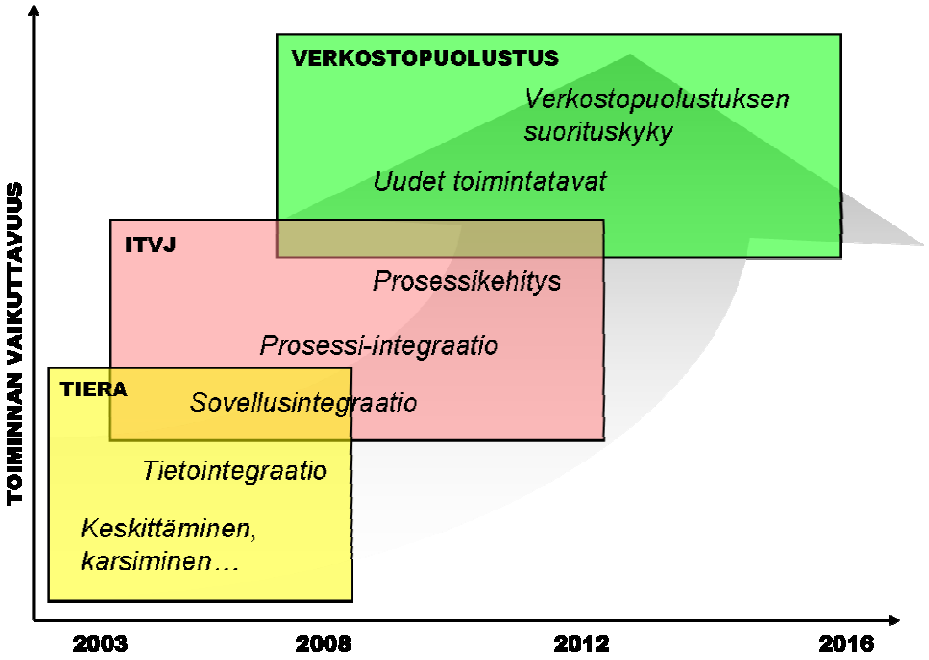
Vuoden 2004 puolustuspoliittisessa selonteossa [44] todetaan, että puolustusvoimille luodaan verkostokeskeisen sodankäynnin asettamat vaatimukset täyttävä, kaikki puolustushaarat kattava yhteinen tiedustelu-, valvonta- ja johtamisjärjestelmä. Tosin selonteossa ei määritellä, mitä verkostokeskeisellä sodankäynnillä tarkoitetaan. Vuoden 2009 selonteossa verkostokeskeisyyttä tai verkostopuolustusta ei mainita lainkaan [45].

Kylkirauta-lehden (3/2006) [7] laajassa verkostopuolustusartikkelissa annetaan verkostopuolustukselle kaksi määritelmää. Vuoden 2004 määritelmän mukaan verkostopuolustus on alueellisen puolustusjärjestelmän kehittämiseen liittyvä käsite, joka kuvaa 2010-luvun kokonaismaanpuolustuksen, alueellisen taistelun ja tehtävätaktiikan toteuttamista yhteiskäyttöisiä tietoja ja tietoverkkoja laajasti hyödyntäen. Määritelmä kuvaa ajattelutavan kaksi keskeistä komponenttia: yhteistoimintaverkostot ja erilaiset tietoverkot. Teknisten viestiverkkojen yhdistämien komponenttien ohella verkostojen muodostumiseen tarvitaan myös inhimillistä kontaktia. Toisen vuonna 2005 tarkennetun määritelmän mukaan verkostopuolustus on alueellisen puolustusjärjestelmän kehittämistä kuvaava työnimi, joka kuvaa, miten tulevaisuuden tietoverkot ja erilaiset verkostot yhdessä kehittyneiden tieto- ja asejärjestelmien kanssa mahdollistavat yhteis- ja alueellisten operaatioiden toteuttamisen sekä viranomaisyhteistoiminnan kokonaismaanpuolustuksen päämäärien saavuttamiseksi.

Puolustusministeriön tietohallintostrategiassa vuodelta 2007 [39] verkostopuolustus määritellään työnimeksi, joka mahdollistaa yhteis- ja alueellisten operaatioiden käskytyksen ja valvonnan sekä viranomaisten välisen yhteistoiminnan Suomen yhteiskunnan elintärkeiden toimintojen turvaamisessa ja kansainvälisessä yhteistoiminnassa. Määritelmä perustuu puolustusvoimain komentajan vuonna 2005 pitämään konferenssiesitykseen. Määritelmää voidaan pitää verkostopuolustuksen virallisena määritelmänä, koska puolustusministeriön tietohallintostrategia on ainoa virallinen asiakirja, joka määrittelee kyseisen termin.

Puolustusvoimissa verkostopuolustus on nähty varsinkin johtamisjärjestelmäalan näkökulmasta tavoitetilana, johon päästään hallitun prosessin avulla [26]. Keskeisimmät prosessin vaiheet ovat olleet tietohallinnon rationalisointihanke (TIERA) sekä integroidun tiedustelun, valvonnan ja johtamisen järjestelmän (ITVJ) rakentamisen aloittaminen. Näillä kehittämishankkeilla on ollut tavoitteena mahdollistaa puolustusvoimien johtaminen 2010-luvun loppupuolella uuden toimintamallin eli verkostopuolustuksen mukaisesti. Kuvassa 4 on esitetty etenemispolku kohti verkostopuolustusta johtamisjärjestelmäalan näkökulmasta. Tavoitteena on kehittää verkostokeskeisiä kykyjä siten, että tavoitetilassa 2010-luvun puolessavälissä puolustusvoimilla on valmiudet verkostopuolustusoperaatioihin. Huomioitavaa on, että verkostopuolustuksen rakentaminen ei ole prosessi, joka päättyy valmiina tavoitevuonna, vaan suorituskykyjen kehittäminen jatkuu sen jälkeenkin.

Informaatio- ja tietoliikennejärjestelmän (vrt. ITVJ) rooli suomalaisessa verkostopuolustuksessa on välillä liiankin korostunut, vaikka sen rooli toimijoiden verkottumisessa on keskeinen. ITVJ-järjestelmäkokonaisuuden tavoitteena on mahdollistaa eri sensoreista ja lähteistä hankitun tiedon kerääminen, analysointi ja fuusioiminen päätöksenteon sekä asejärjestelmien ja joukkojen käytön perustaksi toiminnan kaikilla tasoilla. ITVJ mahdollistaa yhteisesti käytettävissä olevan ja reaaliaikaiseen tilannekuvan koko valtakunnan alueella. ITVJ antaa mahdollisuudet johtaa keskitettyjä, kaikki puolustushaarat käsittäviä yhteisoperaatioita osana alueellista puolustusjärjestelmäämme. Järjestelmällä kyetään vastaamaan myös informaatiosodankäynnin haasteisiin.



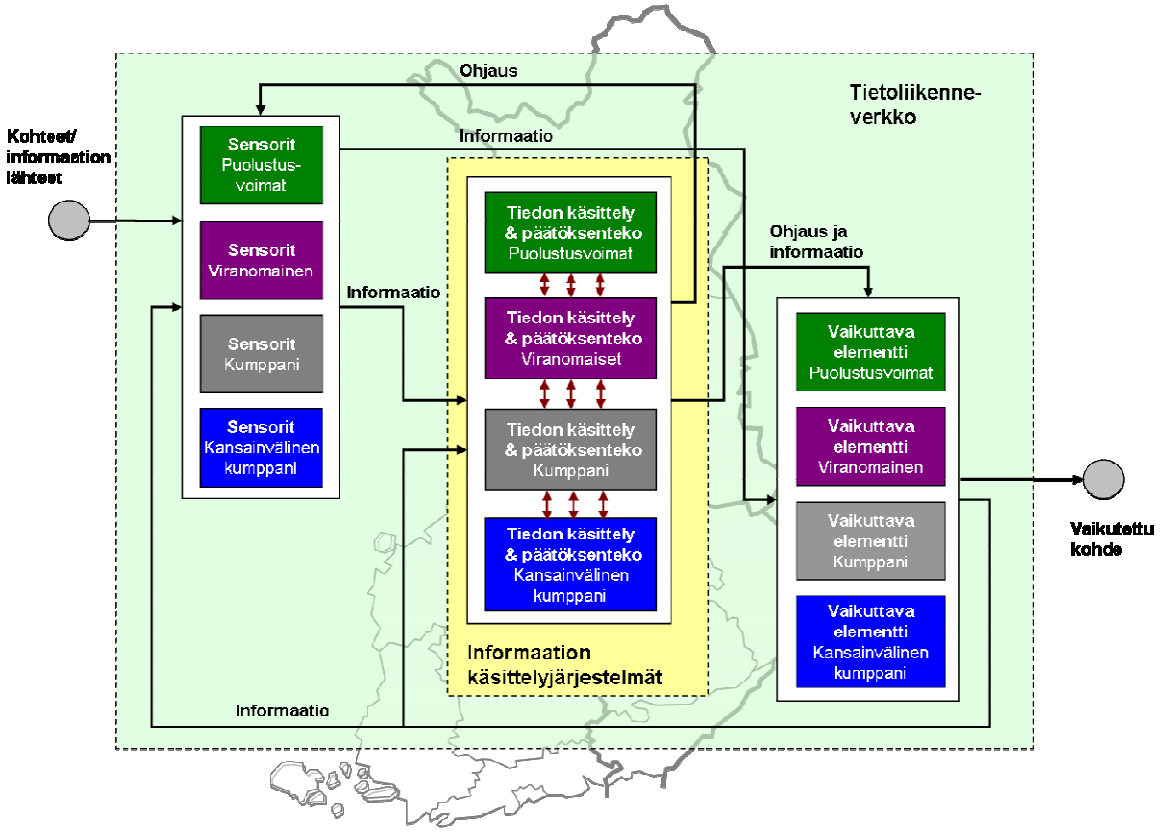
Kuva 4. Verkostopuolustus tavoitetilana.

Edellä mainittuja määritelmiä tarkastellessa voidaan todeta, että suomalaisena konseptina verkostopuolustus on kevyesti määritetty termi, joka kuvaa toiminnan tavoitetilaa ylimalkaisesti. Verkostopuolustuksen prosesseja, tilannetietoisuuden muodostamista ja tiedon jakamisen problematiikkaa ei ole ainakaan julkisten lähteiden perusteella tutkittu ja kehitetty systemaattisesti. Vuonna 2010 alkanut puolustusvoimien strateginen suunnittelu ja tavoitetilatyö 2025 sisältänevät tarkempaa kuvausta ja määrittelyä verkostopuolustuksen toimijoista, organisaatioista, prosesseista, tavoitteista ja teknisistä ratkaisuista.

Suomalaista käsitettä tarkastellessa on syytä huomata, että määritelmä ei ole ristiriidassa alkuperäisen NCW-konseptin suhteen. Informaatioteknologisilla järjestelmillä pyritään edelleen tukemaan tiedon jakamista, jalostamista, nopeampaa päätöksentekoa ja sitä kautta verkostopuolustuksen hyötyjen saavuttamista. Suomalainen määritelmä on jo alun perin huomioinut esimerkiksi viranomais- ja kansainvälisen yhteistyön sekä korostanut verkostokeskeisyyden sosiaalista ulottuvuutta. Nämä seikat ovat tulleet kansainvälisiin käsiitteisiin vasta viime vuosina (vrt. NCO ja Naton *Comprehensive Approach*).

Tulevaisuuden taistelukentällä joukot ja asejärjestelmät ovat entistä pienempiä kokonaisuuksia ja ne toimivat entistä itsenäisemmin. Erillään toimivien yksiköiden vaikutuksen keskittäminen vaatii verkostokeskeistä lähestymistapaa, jonka tärkeimmät tekijät ovat tilannetietoisuus ja varmennetut johtamisyhteydet. Verkottunut kokonaisuus kestää paremmin tappioita ja se kykenee ylläpitämään vaadittavia yhteyksiä ja johtamispaikkoja. Suunnittelu-, päätös- ja

toimeenpanovallan levittäminen kaikille organisaatiotasoille mahdollistaa hajautetun ja taistelunkestävän johtamisen sekä tehokkaan vaikuttamisen.[40]



Kuva 5. Verkostopuolustus – suomalainen paradigma?

Kuvassa 5 on hahmoteltu suomalaista verkostopuolustusparadigmaa, jossa verkostopuolustus sisältää kaikki yhteiskunnan toimijat. Kuvassa on sovellettu verkostokeskeisen sodankäynnin informaatiovuokaaviota [4] suomalaiseen käsitykseen verkostoitumisesta. Yhteiseen informaatioulottuvuuteen tuotetaan dataa kaikkien toimijoiden (puolustusvoimat, viranomaiset, kumppanit) sensoreilla. Verkostopuolustus ei rajoitu pelkästään kansalliseksi toiminnaksi, vaan kansainväliset kumppanit ovat osa verkostoa. Informaatioulottuvuudessa dataa jalostetaan tiedoksi ja ymmärrykseksi. Yhteinen informaatioulottuvuus ei tarkoita välttämättä yhteistä teknistä järjestelmäkokonaisuutta, mutta siellä on kyettävä jakamaan informaatiota kitkattomasti eri toimijoiden järjestelmien välillä sekä muodostamaan yhteistä tilannetietoisuutta. Informaatioulottuvuudessa on kyettävä yhteistä tavoitetta palvelevaan päätöksentekoon. Päätöksenteon tuloksena on voitava vaikuttaa hallitusti kaikilla yhteiskunnan voimavaroilla. Takaisinkytkennällä kuvataan vaikutuksen aiheuttamia muutoksia toimintaympäristössä.

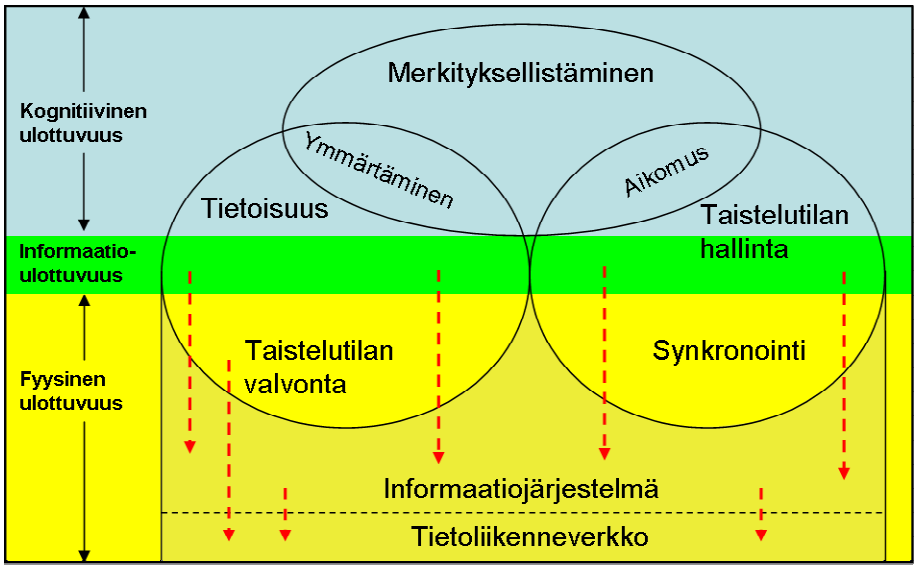
Verkostopuolustuksen konsepti on skaalautuva. Perusoppia voidaan soveltaa strategiselta tasolta aina taktiselle ja jopa taisteluteknisellä tasolle saakka. Verkottumista voi tapahtua kaikil-

la tasoilla eri ulottuvuuksissa. Maavoimien taktisessa perusyhtymässä (prikaati) verkostopuolustus tarkoittaa aselajien ja toimialojen yhteistoimintaa, yhtenäisten prosessien ja toimintatapojen sekä informaatiojärjestelmien yhteentoimivuutta. Yhtymän taktinen tietoliikenneverkko luo teknisen mahdollisuuden verkottaa kaikki yhtymän elementit sekä muut puolustushaarat ja johtoesikunnat.

Taktinen tietoliikennejärjestelmä mahdollistaa kaikkien toimijoiden informaation jakamisen ja yhteisen tilannekuvan muodostumisen. Teknisenä haasteena taktisen tason verkostopuolustusta rakennettaessa on tietoliikennepalvelujen kehittäminen liikkuville joukoille ja jopa yksittäisille sotilaille. Verkostopuolustuksen näkökulmasta taistelukentän kaikissa tilanteissa taktisilla joukoilla pitäisi olla riittävä informaation saavutettavuus, jotta tilannetietoisuuden muodostuminen, päätöksenteko ja toimeenpano onnistuvat halutun vaikutuksen saamiseksi. Informaatioylivoima vastustajaan nähden voidaan saavuttaa vain suhteellisesti paremman tilannetietoisuuden avulla. Liikkuvaa käyttäjää tukevia langattomia teknologioita löytyy runsaasti kaupallisilta markkinoilta, mutta haasteeksi voi muodostua teknologioiden kustannustehokas implementointi. Kaupallisten järjestelmien toimintaympäristön vaatimukset poikkeavat huomattavasti verkostopuolustuksen asettamisista vaatimuksista, jotka varsinkin taktisella tasolla ovat haastavat käyttöympäristön ja toimintatapojen vuoksi.

2.3 Verkostokeskeisyyden vaatimukset tietoliikenteelle

Alkuperäinen verkostokeskeisen sodankäynnin teoria korostaa teknisten verkostojen merkitystä, mutta kuten jo todettiin, nykyinen tutkimus liittää teoriaan entistä voimakkaammin humaanin ulottuvuuden ja prosessit. Teorian kehittyessä tutkimusta on suunnattu muun muassa johtamisen ja suunnittelun prosesseihin [1, 3], jotka muodostavatkin keskeisen osan sotilaallista toimintaa. Informaatioteknologian rooli on tukea ja mahdollistaa näitä prosesseja. Informaatioteknologian kehittämisen näkökulmasta suuntaus on hyvä, koska selkeät prosessit ja toimintatavat tuottavat yksikäsitteisiä vaatimuksia teknisille järjestelmille. Sodankäynnin tekniset järjestelmät on sovitettava sodankäynnin logiikkaan. Kuvassa 6 on esitetty verkostokeskeisen sodankäynnin ulottuvuuksien liittyminen informaatioinfrastruktuurille asetettaviin vaatimuksiin. Pääosa vaatimuksista syntyy informaatiojärjestelmän toiminnallisuudesta. Informaatiojärjestelmä saa taas vaatimuksensa fyysisen ja informaatioulottuvuuden prosesseista ja toimintatarpeista.



Kuva 6. Vaatimusten muodostuminen informaatiojärjestelmälle ja -verkostolle.

Verkostokeskeisen sodankäynnin asettamat vaatimukset tietoliikennejärjestelmille ovat haasteellisia. Ensimmäinen NCW-perusoppi toteaa verkottumisen olevan keskeisin tekijä informaation jakamisen kannalta. Vaikka verkottumista ei rajata pelkästään teknisillä järjestelmillä tapahtuvaan verkottumiseen, voidaan olettaa, että tekniset järjestelmät parantavat verkottumista varsinkin hajautetussa toiminnassa. Verkostoitumisen keskeinen sisältö onkin luoda tietoliikennejärjestelmä, joka kykenee liittämään kaikki taistelukentän sensorit sekä asejärjestelmät käyttäjineen toisiinsa. Lisäksi operaatioiden suunnittelu ja johtaminen vaativat tietovarastojen kytkemistä osaksi verkostoa siten, että sen tietosisältö on kaikkien saatavilla. Tietoliikennejärjestelmän tulisi kyetä välittämään verkoston tietoa luotettavasti läpi koko taistelukentän strategiselta tasolta aina taistelutekniselle tasolle asti.

Tietoliikenteelle asetettavia vaatimuksia voidaan tarkastella NCO-käsitekehikon [18] avulla (kuva 3). Viitteissä [20] ja [37] on määritetty informaation välittämiselle ja käsittelylle viisi suorituskykyaluetta (kollaboraatio, yhteydellisyys, informaation löytäminen, verkonhallinta ja verkkosolmujen liityntävalmius). Kollaboraatio ja informaation löytäminen ovat tietoliikennekerroksen yläpuolella tapahtuvaa tietojenkäsittelyä, joten tietoliikenteen kannalta merkitykselliset suorituskykyalueet ovat:

1. *Yhteydellisyys (engl. Connectivity Capability).* Integroitujen verkostojen kyky, joka mahdollistaa datan ja informaation jakamisen operaatioon osallistuvien kesken.
2. *Verkkosolmujen liityntävalmius (engl. Net-Ready Nodes Capability).* Operatiivisten toimijoiden kyky kytkeytyä verkostoon.
3. *Verkonhallinta (engl. Network Control Capability).* Kyky hallita ja mukauttaa tietoliikenneverkkoja operaatioiden olosuhteiden mukaan.

Verkottuminen (networking) muodostuu siis pelkistetysti verkon solmuista, solmujen välisistä yhteyksistä ja verkonhallinnasta. Verkkoyhteydet mahdollistavat datan siirtämisen verkkosolmujen välillä. Solmut ovat verkon kannalta toiminnallisia kokonaisuuksia, jotka kykenevät käsittelemään ja jakamaan informaatiota muiden solmujen kanssa sekä pystyvät keskinäiseen yhteistoimintaan. Verkottumisella tarkoitetaankin yhteydellisyyttä operaatiossa toimivien kokonaisuuksien (force entities) välillä. Taulukossa 1 on esitetty yllä oleviin suorituskykyihin liittyvät osatekijät ja mittarit sekä niistä johdetut vaatimukset verkostokeskeisiä operaatioita mahdollistavalle tietoliikennejärjestelmälle. Suorituskyvyn osa-alueet, osatekijät ja mittarit ovat viitteiden [18] ja [20] mukaiset. Vaatimukset on johdettu tarkastelemalla yksittäistä osatekijää ja sen merkitystä tietoliikenteen kannalta.

Yhteydellisyys edellyttää, että verkon solmut voivat kommunikoida toistensa kanssa. Kaksi toimijaa tai solmua on kytketty, jos niiden välillä on olemassa joko fyysinen kanava tai jos ne on linkitetty loogisesti. Looginen yhteydellisyys edellyttää, että kaksi solmua pystyvät kommunikoimaan suoraan toistensa kanssa tai epäsuorasti välittävien solmujen kautta. Puhuttaessa toiminnallisista operaatioista tarkastelun kohteena on yleensä looginen yhteydellisyys. Kuitenkin operatiivinen toiminta voi vaatia fyysistäkin yhteydellisyyttä. Yhteydellisyysvaatimukset ovat pääindikaattoreita verkon vuorovaikutustasoa arvioitaessa. Informaatiota tuottavien ja päätöksiä tekevien operatiivisten toimijoiden (solmujen) määrä vaikuttaa merkittävästi vuorovaikutuksen tasoon. Useat yksiköt tai osat voidaan vaatia toimimaan yhdessä tai ne voidaan tuoda nopeasti yhteen ajallisesti ja tilan suhteen, jotta haluttu vaikutus saavutetaan.

Verkonhallinta ja -valvonta ovat erittäin tärkeässä roolissa verkostokeskeisissä operaatioissa. Ilman jonkinlaista keskitettyä valvontaa tai ohjausta ei ole mahdollista yksinkertaisesti rakentaa toimivaa verkostoa ja odottaa, että toimijat käyttävät sitä. Tämä pätee sekä verkkoinfrastruktuuriin että operatiivisiin toimintoihin, jotka käyttävät verkkoa. Keskitetty verkonhallinta ei kuitenkaan tarkoita verkonhallintajärjestelmän keskittämistä esimerkiksi maantieteellisesti, vaan keskitetysti tapahtuva valvonta voidaan teknisesti hajauttaa koko verkon alueelle.

Taulukko 1. Vaatimukset tietoliikenteelle verkostopuolustuksen paradigmassa.

Suorituskyky	Osatekijä ja mittari	Vaatimus tietoliikenteelle
Yhteydellisyys	**Saavutettavuus** Käytössä olevien linkkien määrä operatiivisten toimijoiden solmujen välillä.	Tietoliikenneyhteys kaikkiin toimijoihin (solmuihin) myös liikkeen aikana.
	Kestävyys (robustisuus) Verkon linkkien määrä, jota voidaan katkaista ilman että saavutettavuus katoaa.	Jokainen solmu on liitetty usealla yhteydellä. Käytettävä yhteystyyppi on taistelunkestävä.
	Kapasiteetti Operatiivista toimintaa tukevat linkit, joiden kapasiteetti ylittää minimikapasiteetin (kbps).	Yhteyden kapasiteetti riittää ko. informaatiojärjestelmän tarpeeseen.
	Viive Operatiivista toimintaa tukevat linkit, joiden tiedonsiirtoviive ei ylitä asetettua kynnysarvoa (ms).	Yhteyden viive vastaa palvelutarvetta (puhe, video, data, real-time).
	Linkin turvallisuus Operatiivista toimintaa tukevat linkit, joiden tietoturvan (salaus yms.) taso ylittää määrätyn minimitason.	Yhteyden tietoturvallisuus vastaa informaatiosisällön vaatimuksia (salainen, julkinen)
Verkkosolmujen liityntävalmius	**Kytkeytymisaika** Enimmäisaika, jonka operatiivinen toimija voi allokoida solmun liittämiseksi verkostoon.	Solmu on plug-and-play -tyyppinen. Kytkeytyminen saa kestää vain sekunteja.
	Solmun kapasiteetti Maksimi kaistanleveys, jonka toiminnallinen solmu tarvitsee ollakseen muiden solmujen tai toimijoiden saavutettavissa.	Riippuu solmussa käytetyistä palveluista. Solmun pieni kaistan tarve (kbps) vähentää verkon kokonaiskuormitusta.
	Solmun yhteydellisyys Minimimäärä mediatyyppejä (kenttäradio, langaton, optinen, kupari jne), jonka operatiivinen toiminto vaatii sen solmujen tai toimijoiden kytkemiseksi.	Tietoliikennejärjestelmän on mahdollistettava erilaiset mediatyypit. Pyrittävä pieneen määrään erilaisia tyyppejä.
	Informaation saatavuus Informaatioformaatit (HTML, XML, VMF jne.), joita solmujen tai toimijoiden vaaditaan tukevan operatiivinen toiminnan mahdollistamiseksi. Käytetään myös nimitystä lähettämis- ja hakuvalmius.	Tietoliikennejärjestelmän on tuettava käytettäviä formaatteja. Tavoitteena on yhteinen formaatti. Erityyppiset palvelut voivat vaatia erilaisia formaatteja (puhe, video, data, real-time).
	Solmuturvallisuus Solmujen tai toimijoiden lukumäärä, jotka operatiivinen toiminta vaatii tukevan nykyisiä salausratkaisuja ja käyttäjähallintaa.	Kaikkien solmujen on täytettävä vaadittu tietoliikenteen tietoturvataso.
Verkonhallinta	**Valvonta** Verkonhallinalle asetettu taso, jolla kyetään tunnistamaan merkittävät muutokset verkko-olosuhteissa. Tärkeää on esimerkiksi määrittää, millaiset häiriöt pitää havaita ja kuinka nopeasti havainnot tehdään.	Verkonhallinnalla on kyettävä valvomaan tietoliikenneyhteyksien tilaa.
	Pääsynhallinta Enimmäisaika, jonka operatiivinen toiminta sallii verkonhallinan aktivoida ja deaktivoida käyttäjiä.	Tietoliikenneyhteyksien käyttövaltuushallinnan vasteaika on oltava mahdollisimman pieni.
	Kaistankäytön hallinta Enimmäisaika, jonka operatiivinen toiminta sallii verkonhallinalle taajuuksien uudelleen allokointiin.	Taajuusallokoinnin ja taajuusmuutokset on kyettävä tekemään mahdollisimman nopeasti.
	Uudelleenreititys/-konfigurointi Enimmäisaika, jonka operatiivinen toiminta sallii verkonhallinalle löytääkseen ja aktivoidakseen uuden reitityksen/konfiguroinnin yhteydettömiin solmuihin.	Tietoliikennejärjestelmän on kyettävä automaattiseen uudelleen reititykseen ja toipumiseen.
	Pääsyn turvallisuus Enimmäismääräoperatiivisten toimijoiden laitteistoja, joihin ei voida tunkeutua luvattomasti verkonhallinnan käytäntöjen ja toimintatapojen vuoksi.	Tietoliikennelaitteet on suojattu lavattomalta tunkeutumiselta (fyysinen, verkkohyökkäykset).
	Kapasiteetin hallinta Aika, jonka operatiivinen toiminta sallii verkonhallinnan lisätä ja poistaa verkosta solmuja turvallisuus ja toiminnallisuusvaatimukset huomioiden. Kapasiteetin hallinta sisältää myös tietovarantosolmujen ja muiden verkkojen solmujen hallinnan.	Tietoliikennejärjestelmä mahdollistaa solmujen liittymisen ja poistumisen mahdollisimman pienellä manuaalisella konfiguroinnilla.

Sen lisäksi, että verkkoinfrastruktuurin on oltava kestävä (robusti), toimijoiden on myös voitava liittyä verkkoon operatiivisen toiminnan mahdollistamiseksi. Operatiiviset toimijat on varustettava tarvittavan liittymiskyvyn omaavilla laitteilla. Verkkosolmujen liityntävalmius sisältääkin sekä toimijat itsessään että myös tietoliikennelaitteet, joilla verkkoon voidaan liittyä. Verkon valmiustaso vaikuttaa suoraan verkoston vuorovaikutustasoon. Jotkin operatiiviset toiminnot saattavat edellyttää hyvin vähän suoraa pääsyä verkkoon, mutta toiset saattavat taas vaatia jatkuvaa ja merkittävää pääsyä.

Verkostokeskeisen sodankäynnin asettamat vaatimukset kulminoituvat järjestelmien väliseen yhteensopivuuteen, joka korostuu jo pelkästään puolustusvoimien tehtäviä tarkastelemalla. Verkostopuolustusta tukevan järjestelmän olisi kyettävä toimimaan yhteen niin viranomaisten kuin kansainvälisten yhteistyötahojen kanssa. Yhteensopivuus on merkittävä vaatimus yhteisoperaatioiden suunnittelussa ja johtamisessa. Verkostokeskeinen toiminta tuo yhteistoimintatarpeet erittäin matalalle tasolle, mikä osaltaan vaatii tietoliikennejärjestelmiltä yhteentoimivuutta.

Informaatioinfrastruktuurin luotettavuus ja helppokäyttöisyys ovat perusvaatimuksia. Mikäli tietoverkkoa ei koeta luotettavaksi, sen käyttöä voidaan vähentää tai sitä ei käytetä ollenkaan. Helppokäyttöisyys liittyy myös verkon käyttöintensiteettiin. Helppokäyttöinen järjestelmä koetaan hyödylliseksi, kun taas vaikeaa järjestelmää käytettäessä sitoudutaan järjestelmän oppimiseen eikä sotilasoperaation suunnitteluun tai johtamiseen. Helppokäyttöisyyteen liittyy myös teknisten järjestelmien plug-and-play -ominaisuudet, joilla voidaan nopeuttaa ja helpottaa verkon konfigurointia ja ylläpitoa taistelukentällä.

Tietoliikennejärjestelmien kapasiteetilta vaaditaan yhä enemmän tietojenkäsittelytavan muuttuessa verkostokeskeisissä operaatioissa. Suurikapasiteettinen tietojenkäsittely siirtyy päätelaitteista tietovoimaloihin, joissa tietojenkäsittelystä otetaan tehoja simulointiin, datafuusioon ja ennustamiseen. Käyttäjään integroitu tietojenkäsittelykapasiteetti käytetään vuorovaikutuksen tehostamiseen sekä tilannetietoisuuden parantamiseen. [43]

2.4 Kognitiivinen tietoliikenneverkko

Viime vuosina tietoverkkojen ja tietoliikennejärjestelmien kehittämiseen on liitetty voimakkaasti termit *kognitiivinen* ja *älykäs*, mutta termeille ei ole luotu yleispätevää määritelmää tietoliikenneteknologian näkökulmasta. Yleisesti kuitenkin ymmärretään, että edellä mainitut termit kuvaavat teknologian kykyä mukautua ympäristön muutoksiin [47]. Kielitoimiston sanakirjan [32] mukaan kognitio tarkoittaa tajuntaa ja sen sisältöä kokonaisuutena. Tajuntaan

liittyy kyky havainnoida ja jäsentää ympäristöä, ajattelu, päättely ja ongelmanratkaisu. Kognitiivisissa tietoliikenneverkoissa pyritään hyödyntämään erilaisia tekoäly ja oppimistekniikoita ”tajunnan” synnyttämiseksi. Kognitiivisten verkkojen perustoimintoja ovat havainnointi, oppiminen, päätöksenteko, itseohjautuvuus ja automaattinen konfiguroituminen [29].

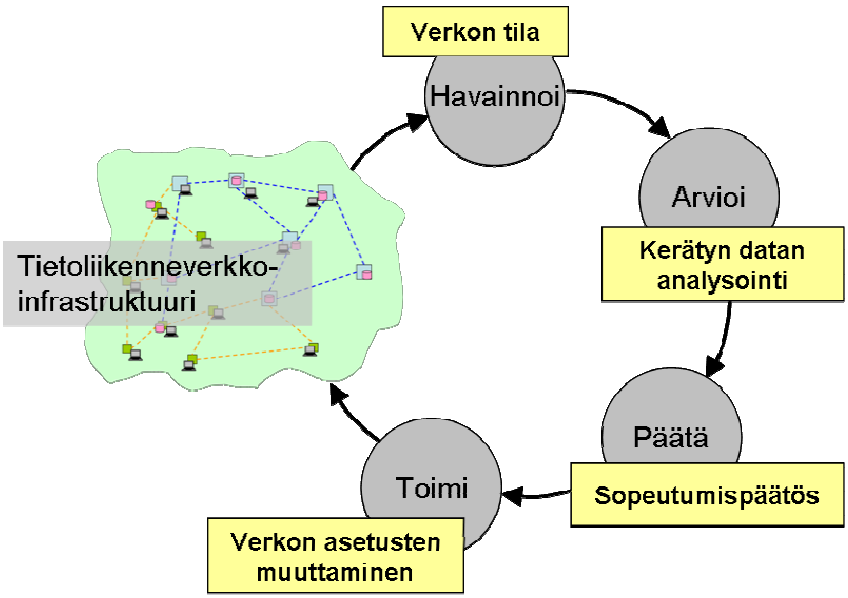
Viitteessä [47] esitetään kognitiiviselle verkolle seuraava määritelmä:
Kognitiivinen verkko sisältää kognitiivisen prosessin, joka kykenee hahmottaan sen hetkiset verkon olosuhteet, jonka jälkeen prosessi suunnittelee, päättää ja toimii näiden olosuhteiden perusteella. Verkko voi oppia näistä mukautumisista ja niitä voidaan käyttää seuraavia päätöksiä tehtäessä. Kaikissa vaiheissa huomioidaan päästä-päähän -tavoitteet.

Määritelmä jäljittelee kognition ja oppimisen perusmalleja. Verkkoon ja päästä-päähän -tavoitteeseen liittyvät näkökulmat ovat kriittisiä tekijöitä, jotka erottavat kognitiivisen verkon muista kognitiivisista viestintäteknologioista. Ilman näitä tekijöitä järjestelmä voi sisältää kognitiivisia osia (esimerkiksi radio-osa), mutta järjestelmä ei ole kokonaisuudessaan kognitiivinen tietoliikenneverkko. Päästä-päähän -termillä tarkoitetaan tässä yhteydessä kaikkia verkon osia, jotka tarvitaan datavirran siirtämiseen. Päästä-päähän -ketju voi muodostua esimerkiksi aliverkoista, reitittimistä, kytkimistä, virtuaaliyhteyksistä, salausjärjestelmistä, siirtomedioista, rajapinnoista tai aaltomuodoista.

Päästä-päähän -tavoite saa aikaan verkon laajuisen kognitiivisen luonteen, mikä toisaalta edellyttää verkkoelementtien olevan ohjelmistopohjaisesti konfiguroitavissa. Käytännössä tämä tarkoittaa, että verkko voi itsenäisesti modifioida eri verkkokerroksia tietoliikenneverkon solmuissa. Esimerkiksi sähköisesti ohjatuilla antenneilla varustettu radio voi muodostaa kognitiivisen verkon, mikäli järjestelmä on tietoinen antennin ohjauksen vaikutuksesta päästä-päähän -tavoitteeseen. Radioista ei muodosta kognitiivista verkkoa, jos radiojärjestelmä on tietoinen vain antennin konfiguroinnin muutoksen vaikutuksesta linkin laatuun, eikä esimerkiksi tiedosta muutoksen vaikutusta muihin verkon solmuihin.

Kognitiivisen verkon oppimisprosessi perustuu lähes kaikkien oppimismallien sisältämä palautesilmukkaan, joka muodostuu aiemman ympäristövuorovaikutuksen ohjatessa sen hetkistä tai tulevia päätöksiä. Kuva 7 havainnollistaa yksikertaista esimerkkiä palautesilmukasta, jonka alun perin esitti jo aiemmin mainittuna OODA-silmukkana J. Boyd [9]. Kognitiivinen järjestelmä tarkkailee ympäristöään ja verkon tilaa, minkä jälkeen järjestelmä arvio ja analysoi verkon ja ympäristön tilaa suhteessa haluttuun tavoitetilaan. Päätösvaiheessa tietoliikenneverkko päättää, miten verkon asetuksia muutetaan. Lopuksi säädetään verkon parametrit ja havain-

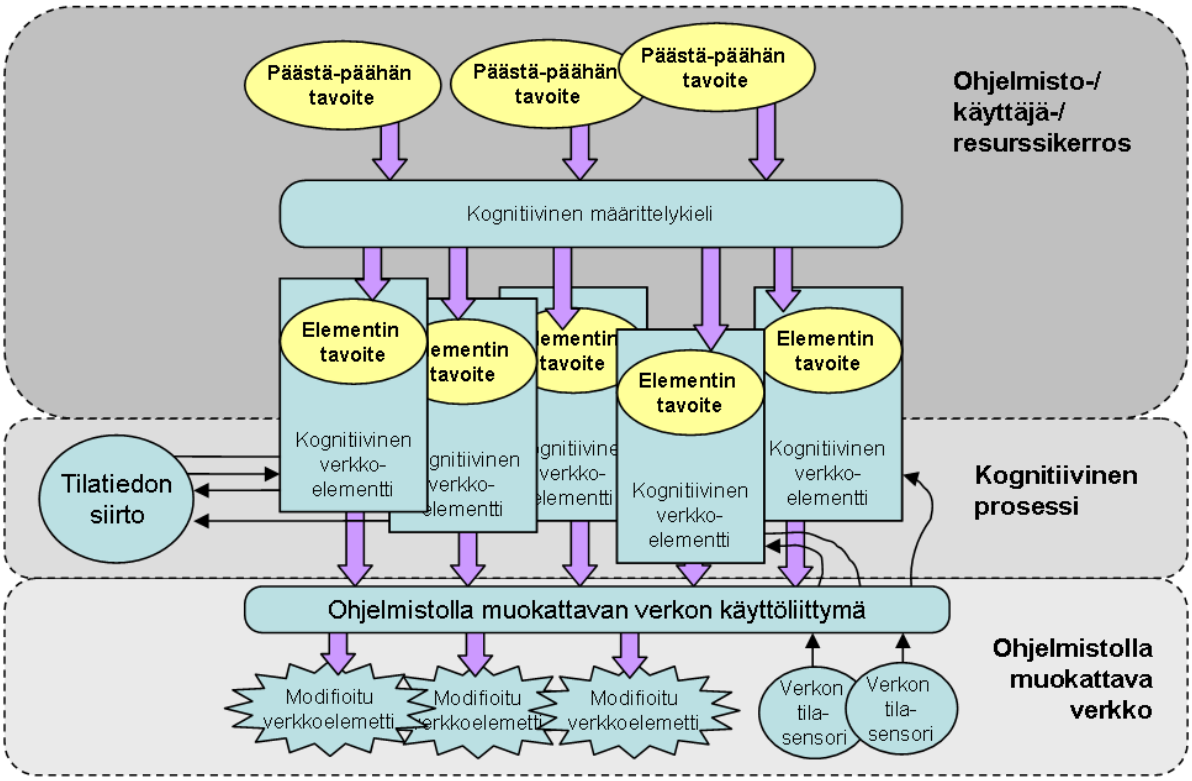
noidaan muutoksen vaikutusta. Oppiminen on tärkeä osa silmukkaa, koska sillä voidaan estää aiempien virhevalintojen uusiutuminen tulevissa päätöksissä.



Kuva 7. Kognitiivisen tietoliikenneverkon palautesilmukka (OODA-silmukka).

Kognitiivista verkoista on luotu useita malleja, joissa tietoliikenneverkkoon lisätään kognitiivinen kerros tai taso. Heikkoutena malleissa on ollut kognitiivisen prosessin kytkeminen koko verkon laajuiseksi toiminnaksi. Lähteessä [49] on esitetty kognitiivisen tietoliikenneverkon kolmikerroksinen malli, jonka ylin kerros muodostuu järjestelmän ja verkkoelementtien tavoitteista, jotka määrittävät verkon käyttäytymistä. Nämä tavoitteet ovat syötteenä kognitiiviselle prosessille, joka määrittää järjestelmän suorittamat toimenpiteet. Mallin alimmalla kerroksella on ohjelmistolla muokattava verkko (*engl. Software Adaptable Network, SAN*), joka sisältää järjestelmän fyysisen ohjauksen ja toimii kognitiivisen prosessin toimintaulottuvuutena. Kuvassa 8 on havainnollistettu edellä kuvattu malli.

Kognitiivinen prosessi koostuu yhdestä tai useammasta kognitiivisesta elementistä, jotka toimivat autonomian ja täyden yhteistyön välimaastossa. Yksittäinen kognitiivinen elementti voi olla fyysisesti jakaantunut yhteen tai useampaan verkon solmuun. Useita kognitiivisia elementtejä voi olla jakaantunut verkon solmujen kesken tai ne voivat sijaita kaikki samassa solmussa. Näin kognitiiviset elementit toimivat kuten ohjelmistoagentit [49].

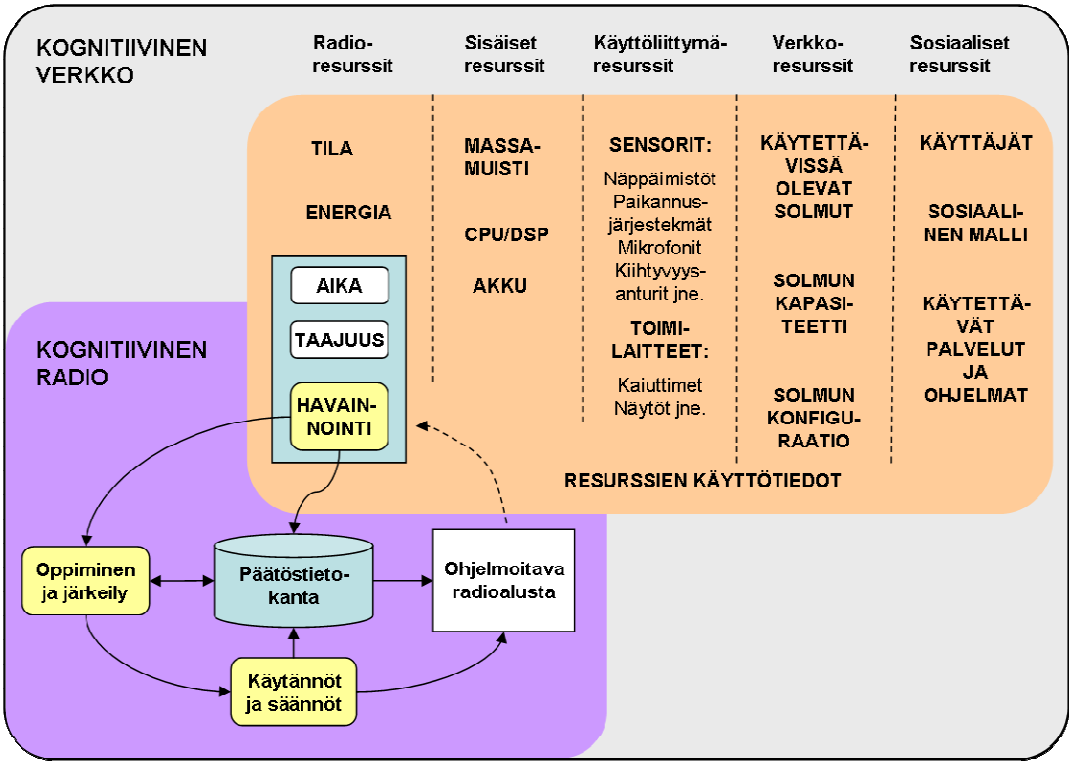


Kuva 8. Kognitiivisen verkon perusrakenne.

Verkon käyttäjien päästä-päähän -tavoitteiden kytkemiseksi kognitiiviseen prosessiin tarvitaan käyttöliittymä. Kuvan 8 mallissa tämä tapahtuu kognitiivisen määrittelykielen (*engl. Cognitive Specification Language, CSL*) avulla. Määrittelykieli ohjaa kognitiivisten elementtien toimintaa kääntämällä päästä-päähän tavoitteet paikallisten elementtien tavoitteiksi. Mallin mukaan kognitiivinen prosessi voidaan mieltää koneoppimiseksi, jolloin prosessissa voidaan hyödyntää erilaisia tekoälyyn, päätöksentekoon ja mukautuviin algoritmeihin liittyviä tekniikoita. Kognitiivisen kerroksen toiminta perustuu informaation määrään ja tietoisuuteen, jolloin keskeinen haaste on informaation tehokas jakaminen verkon solmujen välillä. Informaation jaossa joudutaan optimoimaan kaistan ja prosessorien käytön suhdetta saavutettavaan hyötyyn. Laajojen ja monimutkaisten tietoliikenneverkkojen kognitiivisessa toiminnassa joudutaan hyväksymään myös epätietoisuus päätöksenteossa.

Ohjelmoitava verkko (SAN) muodostuu sovelluskäyttöliittymästä (engl. *Application Programming Interface, API*), muokattavista verkkoelementeistä ja verkon tilaa mittaavista antureista. SAN ei kuulu varsinaisesti kognitiivisten verkkojen tutkimusalueeseen, mutta kognitiivisen prosessin tulee olla tietoinen API:sta ja rajapinnoista. Kaikki verkon elementit eivät välttämättä ole muokattavia, mikä on huomioitava kognitiivisessa kerroksessa. Verkon tilaa voidaan havainnoida paikallisesti (esim. kaistanleveys, akun kesto) tai laajemmin (esim. päästä-päähän -viive, topologia).

Sodankäynnin taktisella tasolla tietoliikenneyhteydet on tyypillisesti toteutettu radioyhteyksillä, jolloin informaatio- ja johtamisjärjestelmän käyttö ja tiedon jakaminen on mahdollista myös liikkeen aikana. Kognitiivinen radioverkko muodostuu kognitiivisista radioista ja verkon suorituskyky kulminoituu radion kykyyn hyödyntää sähkömagneettista spektriä mahdollisimman tehokkaasti. Kognitiivinen radioverkko voidaan määrittää konseptiksi, jossa langattomat solmut säätävät ominaisuuksiaan ja asetuksiaan saavuttaakseen mahdollisimman tehokkaan ajallisen ja paikallisen spektrinkäytön. Säätäminen perustuu radion, taajuusympäristön, säännöstön (*engl. policy*) sekä korkeamman tason asettamiin vaatimuksiin, ja se tapahtuu luonnollisesti jatkuvan oppimisen avulla [53]. Kuvassa 9 on esitetty kognitiivinen radio osana kognitiivista verkkoa [53]. Kognitiivisuutta tarkastellaan verkon resurssien näkökulmasta [23].



Kuva 9. Kognitiivinen radio osana kognitiivista verkkoa [23].

Kognitiivisen radion tärkein elementti on päätöstietokanta, jonka perusteella aiempi käytös voidaan ottaa osaksi analysointia ja päätöksentekoa. Kognitiivisen prosessin kannalta hallittavat resurssit vaihtelevat yksittäisen radion resursseista aina verkkotason resursseihin ja käytettäviin palveluihin asti. Kognitiivinen prosessi pyrkii optimoimaan verkon resurssien käytön vaaditun tavoitteen saavuttamiseksi.

Vaikka kognitiivinen toiminnallisuus soveltuu kaikentyyppisiin verkkoihin, sotilastietoliikenteen näkökulmasta tarkasteltuna suurin tarve kognitiiviselle verkolle on taktisella tasolla, jossa verkko on tyypillisesti erittäin dynaaminen ja muutoksia tapahtuu jatkuvasti. Luonnollinen ympäristö kognitiivisen toiminnallisuuden implementoinnille on taktinen radioverkko, jolla pyritään tarjoamaan tietoliikennepalvelut liikkuville joukoille tai yksilöille. Kognitiivinen verkko vapauttaa radioverkkojen ylläpitoresursseja, ja toisaalta automaattisesti mukautuvassa verkossa manuaalisesta ylläpidosta johtuvien virheet poistuvat.

2.5 Kognitiivisen verkon perusominaisuudet

Perusolettamus on, että kognitiivinen verkko tarjoaa paremman päästä-päähän -suorituskyvyn kuin perinteinen, ei-kognitiivinen tietoliikenneverkko [47]. Kognitiivisella prosessilla voidaan parantaa verkon resurssien hallintaa, palvelun laatua (*engl. Quality of Service, QoS*), turvallisuutta, kulunvalvontaa, pääsynhallintaa ja monia muita verkolle määritettyjä tavoitteita. Kognitiivisen verkon toimintaa rajoittaa ainoastaan verkkoelementtien kyky mukautua. Ideaalinen kognitiivinen verkon toiminta on ennakoivaa eikä reaktiivista, jolloin mukautuminen tapahtuu jo ennen kuin varsinainen ongelma ilmenee.

Kognitiivisella verkolla on kolme perusominaisuutta: tilannetietoisuus, oppimis- ja päätöksentekokyky sekä täysin kontrolloitavat tietoliikenneparametrit ja -asetukset [29]. Tilannetietoisuus syntyy verkon kyvystä havainnoida ympäristöä ja verkon tilaa ja muodostaa siten käsitys vallitsevista olosuhteista. Verkon optimoinnin kannalta on tärkeää, että verkkosolmut jakavat tilatietonsa muiden solmujen kanssa. Kognitiivisissa radioverkoissa merkittävä tekijä on sähkömagneettisen spektrin aistiminen ajallisesti tai paikallisesti vapaiden radiokanavien löytämiseksi. Oppimiskyky muodostuu verkon kyvystä oppia aiemmista tapahtumista ja päätöksentekokyky taas tarkoittaa verkon kykyä tehdä päätöksiä tilannetietoisuuteen ja oppimiseen perustuen.

Oppimis- ja päätöksentekoprosessissa verkkosolmun käyttäytyminen voi vaihdella puhtaasti itsekkäästä ja individuaalisesta sosiaaliseen ja epäitsekkääseen. Vaikka epäitsekäs ja sosiaalinen käyttäytyminen saattaa tuntua luonnolliselta päästä-päähän -vaatimuksia tavoiteltaessa, solmun itsekäs käyttäytyminen voi joskus olla tehokas tapa verkon sopeuttamisessa [46]. Itsekäs verkon käytös voi olla järkevää, koska reaalimaailmassa tietoliikennejärjestelmien solmut eivät usein ole globaalin hallinnan piirissä. Lisäksi solmun itsekkyys vaatii vähemmän keskitettyä koordinointia, mikä vähentää tietoliikenteen kuormaa. Itsekkyyttä voidaan tarkastella kaavan (1) avulla [47]. Verkkoelementin toiminta on itsekästä, kun elementin i seuraavan

toimenpiteen hyöty u_i on suurempi kuin elementin i sen hetkisen toiminnan hyöty. Tällöin oletetaan muiden elementtien toimivan, kuten elementti i kuvittelee (merkitään $a_i^{\sim t+1}$) [47]

$$u_i\left(a_i^{t+1}, a_{-i}^{\sim t+1}\right) \geq u_i\left(a_i^{t}, a_{-i}^{\sim t+1}\right) \tag{1}$$

”Uskomus” kaavassa (1) on tärkeä, koska tietämättömyys muista voi tehdä elementin toimintavektorista erilaisen kuin mitä muissa elementeissä ilmenevä todellinen toiminta tekisi. Verkon voidaan sanoa toimivan *itsekkäästi*, kun jokainen elementti valitsee vain ne toimenpiteet, jotka jatkuvasti parantavat vain elementin omia tavoitteita. Epäitsekäs verkko yrittää saavuttaa päästä-päähän -tavoitteet. Kustannusfunktio C kvantisoi verkon suorituskyvyn kunkin toimintavektorin a suhteen. Verkon toiminta on epäitsekästä, kun elementti pienentää sen hyödyn pienentääkseen kustannusfunktiota. Toiminta on epäitsekästä, kun seuraavat pätevät [47]:

$$\begin{aligned} u_i\left(a_i^{t+1}, a_{-i}^{\sim t+1}\right) &< u_i\left(a_i^{t}, a_{-i}^{\sim t+1}\right) \\ C_i\left(a_i^{t+1}, a_{-i}^{\sim t+1}\right) &\leq C\left(a_i^{t}, a_{-i}^{\sim t+1}\right) \end{aligned} \tag{2}$$

Verkon voidaan sanoa toimivan *epäitsekkäästi*, kun ainakin yksi solmu toimii epäitsekkäästi jossakin kohtaa päätöksentekoketjua.

Päätöksenteon perustana oleva informaatio ei ole aina täydellistä ja päätöksenteon laskennassa on hyväksyttävä informaatiopuutteet. Informaatiopuute voi tarkoittaa, että solmut eivät tiedä tarkkaan muiden solmujen tavoitteita tai käytöstä. Muuttuja Y_i määrittää sen signaalijoukon, jonka elementti i tarvitsee oppiakseen kaikkien verkkoelementtien toiminnan (elementti i mukaan lukien). Todennäköisyys, että toiminta $\mathbf{a}$ oli tapahtuma, joka aiheutti signaalin $y_i \in Y_i$, voidaan merkitä $P\left[\mathbf{a}\middle|y_i\right]$. *Epätietoisuus* [47] ilmenee, kun

$$\exists y_i \in Y \text{ siten, että } P\left[\mathbf{a}\middle|y_i\right] < 1 \,\forall\, \mathbf{a} \in A \tag{3}$$

.

Epätietoisuus vallitsee, kun ainakin yksi verkon solmuista tekee päätöksen epätietoisesti. Epätietoisuus voi johtua epävarmasta tai puuttuvasta tiedosta tai tiedosta, joka ei ole yksikäsitteinen. Mikäli verkossa ei ilmene epätietoisuutta voidaan sanoa, että verkolla on *täysi tietämys*, jolloin voidaan määrittää [47]

$$\exists \mathbf{a} \in A \text{ siten, että } P\left[\mathbf{a}\middle|y_i\right] = 1 \,\forall\, y_i \in Y \tag{4}$$

Täysi tietämys edellyttää, että kakki verkkoelementit tekevät tietoisia päätöksiä kaikissa päätöksenteon vaiheissa.

Täysin kontrolloitavat eli ohjattavat verkon elementit ovat edellytys kognitiivisen verkon maksimaaliselle suorituskyvylle. Ideaalisessa tilanteessa kaikki verkkoelementit ja parametrit ovat kognitiivisen kerroksen ohjattavissa. Tällöin verkko voidaan optimoida täydellisesti kuhunkin tilanteeseen eli päästä-päähän -tavoitteeseen. Esimerkiksi, jos muunneltava kohde on radion lähetysteho, täydellinen kontrolli tarkoittaa, että jokaisen radion lähetystehoa ohjaa kognitiivinen elementti. Jos k on muunneltavien parametrien määrä koko verkossa, ja x on niiden parametrien määrä, joita ohjaa kognitiivinen prosessi, *täydellinen kontrolli* [47] ilmenee, kun

$$\frac{x}{k} = 1 . \tag{5}$$

Verkolla on *osittainen kontrolli* [47], kun

$$\frac{x}{k} < 1 . \tag{6}$$

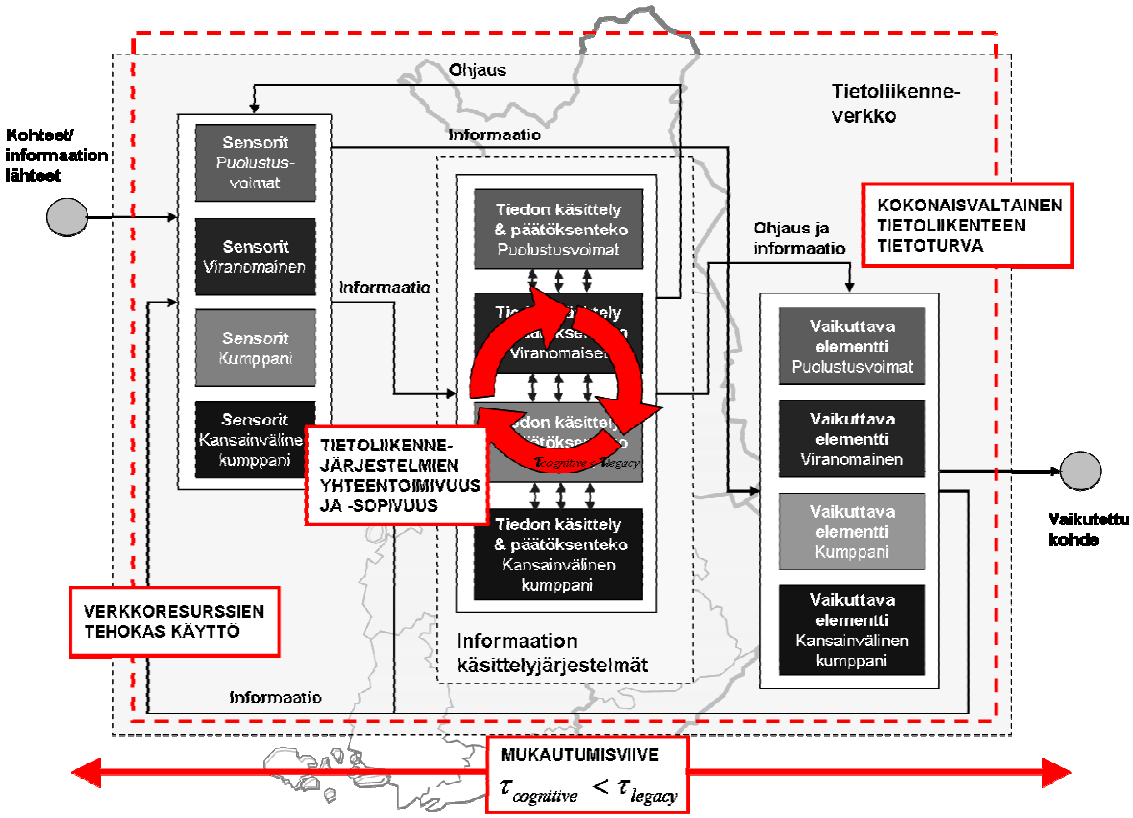
2.6 Johtopäätökset

Verkostokeskeisen sodankäynnin paradigman keskeisin tekijä on ihmisten, prosessien, tiedon lähteiden ja tietojärjestelmien verkottuminen. Vaikka verkostokeskeisyys on suurimmalta osin muuta kuin teknistä verkottumista, tietoliikennejärjestelmällä on tärkeä rooli informaation jakamisen mahdollistajana. Toimiva ja kattava tietoliikennejärjestelmä mahdollistaa informaation nopean, turvallisen ja oikea-aikaisen liikkumisen verkostokeskeisten toimijoiden välillä. Ilman tietoliikenne järjestelmää tiedonkäsittelyjärjestelmien hyöty voi olla minimaalinen.

Suomalaisessa verkostopuolustuksen paradigmassa verkoston toimijoita ovat kaikki yhteiskunnan elintärkeiden toimintojen rakentamisessa ja ylläpidossa tarvittavat yhteisöt. Haasteena on verkottaa nämä toimijat luotettavasti ja turvallisesti sekä kehittää toimijoiden prosessit ja toimintatavat tukemaan verkostokeskeisiä prosesseja. Tietoliikenteen kannalta keskeisiä haasteita ovat järjestelmien yhtyeentoimivuus, tietoturva, liikennepolitiikka ja verkonhallinta. Staattisessa tilanteessa verkostot kyetään muodostamaan manuaalisilla prosesseilla, joita yleensä edeltävät usein pitkätkin neuvottelut ja sopimiset. Dynaamisessa tilanteessa palvelu-

tarpeissa tapahtuvat nopeat muutokset aiheuttavat vaatimuksia tietoliikenneverkon kyvylle mukautua nopeasti vallitseviin vaatimuksiin.

Kognitiiviset verkot tuovat uuden näkökulman sotilaallistenkin tietoliikennejärjestelmien kehittämiseen. Tulevaisuudessa tällaisella älykkäällä verkolla kyetään täyttämään paremmin taistelukentän asettamat vaatimukset tietoliikenteelle. Kuvassa 10 on havainnollistettu kognitiivisen verkon tuomaa lisäarvoa verkostopuolustuksen paradigmaan. Teknisen suorituskyvyn näkökulmasta voidaan nostaa esille neljä lisäarvotekijää.



Kuva 10. Kognitiivisen verkon tuoma lisäarvo verkostopuolustuksen paradigmassa.

Ensimmäinen tekijä on aika. Kognitiivinen, automaattisesti mukautuva verkko kykenee vastaamaan nopeasti verkon vaatimiin muutoksiin, joita aiheutuu ensisijaisesti joukkojen ja toimijoiden liikkeestä ja tilannetietoisuuden muodostamisesta taistelukentällä. Kognitiivisen verkon avulla voidaan pienentää manuaalisesta verkon suunnittelusta ja konfiguroinnista aiheutuvaa viivettä. Nopeampi verkon konvergoituminen nopeuttaa yhteyden muodostumista ja edelleen tiedon jakamista joukkojen ja toimijoiden välillä.

Toinen tekijä on tietoturva. Kognitiivinen järjestelmä kykenee ottamaan huomioon tietoturvavaatimukset koko tietoliikenneverkon laajuisesti. Verkko kykenee mukauttamaan tietoturvamekanismien parametrit päästä-päähän -tavoitteiden mukaisesti. Asetettua tietoturvakäytäntöä

noudattava verkko mukautuu automaattisesti, jolloin inhimillisten virheistä ja huolimattomuuksista johtuvat tietoturvapuutteet minimoituvat. Taktisessa langattomassa tietoliikenneverkossa turvallisuutta parantaa edelleen mahdollisuus mukauttaa radioantennien suuntakuviot elektronisen sodankäynnin vaatimusten mukaisesti. Älykkäät antennit säteilevät vain halutuun suuntaan suuntakuvion nollakohtien osoittaessa uhkan suuntaan.

Kolmas tekijä on heterogeenisten tietoliikennejärjestelmien yhteentoimivuus. Verkostopuolustuksen maksimaalisen tehokkuuden saavuttaminen ei onnistu ilman toimijoiden tietoliikennejärjestelmien yhteentoimivuutta. Yhteentoimivuuden tärkeys korostuu viranomaisten ja kansainvälisten toimijoiden yhteisissä operaatioissa. Kognitiivinen prosessi mahdollistaa erilaisilla teknologioille toteutettujen järjestelmien yhteensopivuuden. Radioverkoissa tämä tarkoittaa esimerkiksi aaltomuotojen muokkaamista, siten että solmut eivät häiritse toisiaan. Kognitiivinen prosessi mahdollistaa erityyppisillä järjestelmillä varustettujen toimijoiden välisen kommunikoinnin. Yhtyeentoimivuuden parantuminen lisää myös verkon solmujen saavutettavuutta. Mitä enemmän solmut ovat yhteensopivia, sitä laajemmalta alueelta solmuja voidaan saavuttaa. Verkkojen väliset yhdyskäytävät muuttuvat kognitiivisessa verkossa läpinäkyviksi, jolloin informaation siirtyminen verkon osasta toiseen on mahdollista ja informaation laadussa ei tapahdu heikennystä.

Neljäs tekijä, johon kognitiivinen verkko vaikuttaa verkostopuolustuksen tietoliikenneinfrastruktuurissa, on verkkoresurssien tehokkaampi käyttö. Taktisessa tietoliikenneverkossa tämä tarkoittaa erityisesti sähkömagneettisen spektrin tehokasta käyttöä. Nykyiset kenttäradiojärjestelmät hyödyntävät taajuusspektriä vain osittain. Kognitiivinen radioverkko pystyy tunnistamaan ja hyödyntämään käyttämättömät spektrin osat. Dynaaminen spektrin käyttö tulee olemaan tärkeä kyky tulevaisuudessa, kun pelkästään sotilaskäyttöön osoitetut taajuusalueen vähenevät kaupallisten lupien ja tarpeen myötä. Kognitiivisen verkon verkkoresurssien tehokas käyttö ei rajoitu pelkästään tehokkaaseen taajuuksien käyttöön, vaan kognitiivinen verkko pystyy käyttämään tehokkaasti esimerkiksi saatavilla olevia tietoliikennelinkkejä ja protokollia. Verkkoresurssien tehokas käyttö tarkoittaa myös sitä, että tietoliikennepalveluille ei varata ylikapasiteettia tai -resurssia.

Kognitiivisen prosessin ominaisuuksia voidaan tarkastella verkon solmun itsekkyyden, tietoisuuden ja ohjattavuuden asteen suhteen. Verkostopuolustuksen tehokkuuden näkökulmasta on pyrittävä minimoimaan verkkosolmun itsekkyys, jotta verkon mukautuminen saavuttaa verkonlaajuiset tavoitteet. Toisaalta on pyrittävä maksimoimaan verkkosolmun tietoisuus ja oh-

jattavuus, jotta verkon päätökset ovat mahdollisimman oikeita ja että tehdyt muutospäätökset voidaan toteuttaa kaikissa solmuissa ja verkkokerroksilla.

3 TAKTISEN TIETOLIIKENNEVERKON SUORITUSKYVYN PARANTAMINEN KOGNITIIVISEN PROSESSIN AVULLA

Tutkimuksen toisessa osiossa tutkitaan taktisen tietoliikennejärjestelmän teknisen suorituskyvyn parantamista lisäämällä verkkoon kognitiivista toiminnallisuutta. Tietoliikenneverkon tekninen suorituskyky (*engl. performance*) kuvaa verkon teknisiä ominaisuuksia ja kykyä tuottaa käyttäjien ja tietojärjestelmien asettamien vaatimusten mukaiset tietoliikennepalvelut. Tietoliikenneverkon tekninen kokonaissuorituskyky muodostuu fyysisen kerroksen sekä linkki- ja verkkokerrosten ominaisuuksista, joten kokonaissuorituskyvyn vertailu on erittäin monimutkaista ja haastavaa. Tässä työssä ei pyritä vertailemaan nykyisen ja kognitiivisen verkon kokonaissuorituskykyä, vaan tarkoituksena on osoittaa yksittäisiä tietoliikenneverkon ominaisuuksia analysoimalla kognitiivisen prosessin tuottama lisäarvo taktisen tietoliikennejärjestelmän suorituskykyyn.

Vertailtavat tietoliikenneverkon ominaisuudet on valittu edellisen osion johtopäätösten perusteella (kuva 10). Ominaisuuksia ei ole valittu tarkasti analysoimalla, eikä valittujen ominaisuuksien paremmuutta tai merkitystä ole tarkasteltu. Tavoitteena on ollut löytää yksikertaisia langattoman tietoliikenneverkon yleisiä tekniseen suorituskykyyn liittyviä ominaisuuksia, joilla voidaan esimerkinomaisesti havainnollistaa kognitiivisen tietoliikenneverkon suorituskykymahdollisuuksia.

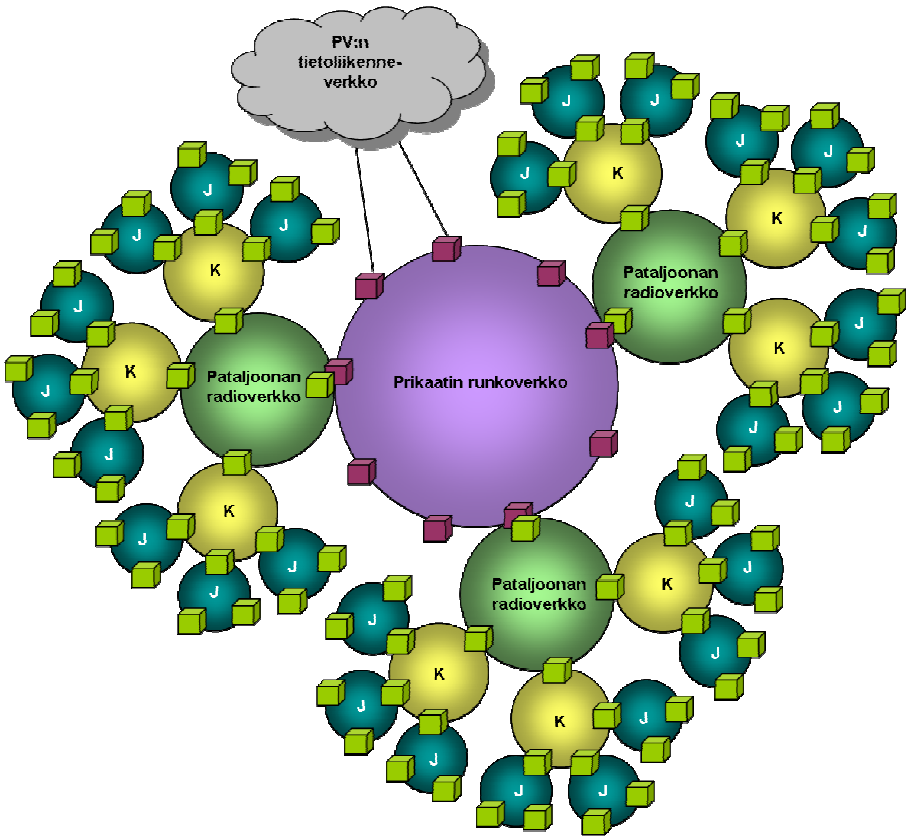
Tietoliikenneverkon suorituskykyä tarkastellaan pelkästään teknisestä näkökulmasta. Analyysissä ei huomioida esimerkiksi kustannustekijöitä, ylläpidon haasteita tai implementointimahdollisuuksia. Analyysissä ei myöskään tarkastella kognitiivisen järjestelmän havainnointi-, analysointi- ja päätöksentekokykyä, vaan tässä yhteydessä oletetaan, että kognitiivinen prosessi toimii optimaalisesti ja että se kykenee hyödyntämään tietoliikennejärjestelmän ominaisuuksia täysimääräisesti koko ajan.

Osio rakentuu neljästä alaluvusta. Ensimmäisessä alaluvussa määritetään taktisen tietoliikenneverkon yksinkertainen malli, joka toimii pohjana ominaisuuksien vertailulle. Toisessa alaluvussa esitetään neljä vertailtavaa tietoliikenneverkon ominaisuutta. Kolmannessa alaluvussa tehdään analyysiä kustakin ominaisuudesta ja viimeinen alaluku sisältää johtopäätökset.

3.1 Taktisen tietoliikenneverkon malli

Yleisellä tasolla tietoliikenneverkko muodostuu verkon solmuista ja niiden välisistä tiedonsiirtoyhteyksistä. Taktisella tasolla tietoliikenneverkon solmuina toimivat erilaiset taktiset reitittimet (laite tai ohjelmisto päätelaitteessa). Tietoliikenneyhteydet on tyypillisesti toteutettu digitaalisilla HF- ja VHF-kenttäradioilla, radiolinkeillä sekä kupari- ja valokuitukaapeleilla [51]. Liikkuvuusvaatimusten kasvaessa kaapeleiden käyttö on vähentynyt merkittävästi. Suurta liikkuvuutta vaativissa taktisen tason operaatioissa kaapeleita ei käytännössä pystytä rakentamaan ollenkaan, vaan yhteydet toteutetaan täysin langattomasti.

Kuvassa 11 on esitetty taktisen tietoliikenneverkon pelkistetty malli. Mallin pohjana on maavoimien perusyhtymä eli prikaati, jossa on kolme pataljoonaa, joissa jokaisessa on kolme komppaniaa. Komppaniassa on edelleen kolme joukkuetta, joissa on kolme ryhmää. Malliin ei ole sisällytetty tukevien aselajeja tai muita joukkoja, koska nykyisen taktisen verkon ja kognitiivisen verkon suorituskyvyn karkeaan vertailuun soveltuu pelkistetty malli. Tietoliikenneverkon ominaisuuksien tarkastelu ja analysointi voidaan toteuttaa riittävällä laajuudella kuvan 11 mukaisella mallilla.



Kuva 11. Taktisen tietoliikenneverkon pelkistetty malli.

Mallista ilmenee hyvin verkon solmujen hierarkkinen rakenne. Ylimmällä tasolla ovat prikaatin runkoverkon muodostavat solmut. Datansiirto eri tason aliverkkojen välillä tapahtuu yhdyskäytäväsolmujen (*engl. gateway, GW*) kautta. Yhtymän tietoliikenneverkko on liitetty ylemmän johtoportaan järjestelmään vähintään yhden solmun kautta, mutta tyypillisesti liityntä on kahden solmun kautta, jolloin vältetään yksittäistä vikaantumispistettä. Kuvan 11 mukaisen verkon toiminta-alueen laajuus riippuu yhtymän operaation luonteesta, mutta tyypillisesti verkko muodostuu noin 10 x 15 km suuruiselle alueelle.

3.2 Vertailtavat tietoliikenneverkon ominaisuudet

Tutkimuksen ensimmäisen osan johtopäätöksissä todettiin kognitiivisen toiminnallisuuden parantavan tietoliikenneverkon neljää ominaisuutta (kuva 10), jotka ovat verkon mukautumisviive, verkkoresurssien käyttö, kokonaisvaltainen tietoturva ja yhteentoimivuus. Näistä mukautumisviive valittiin sellaisenaan yhdeksi vertailtavaksi ominaisuudeksi, koska mukautumisviive voidaan laskea yksinkertaisesti tarkastelemalla manuaalisen ja automaattisen (kognitiiviseen) tietoliikennejärjestelmän verkkomuutosten tekoon vaadittavaa aikaa.

Tietoliikenneverkon resurssien käyttöä voidaan tarkastella kokonaisvaltaisesti tai yksittäisen resurssin suhteen. Kokonaisvaltainen tutkiminen ei ole mielekästä tutkimuksen laajuuden kannalta, joten resurssien käyttöä päädyttiin tarkastelemaan spektrinkäytön tehokkuuden näkökulmasta. Langattomia tietoliikennejärjestelmiä käytettäessä spektrinkäytön tehokkuus on tärkeä ominaisuus, koska sähkömagneettinen spektri on rajallinen resurssi, eikä sitä ole mahdollista hankkia lisää. Spektrinkäytön tehokkuus mittaa langattoman tietoliikennejärjestelmän tiedonsiirtokapasiteettia kaistanleveyden, tilan ja ajan suhteen.

Kokonaisvaltaisen tietoturvan analysointi on erittäin monimutkainen ja haasteellinen prosessi, koska tietoturva muodostuu usean verkkokerroksen toiminnan ja teknisen ratkaisun tuloksena. Tutkimuksen laajuus ei mahdollista kognitiivisen verkon kokonaisvaltaisen tietoturvan teoreettista tarkastelua. Tietoturvaominaisuuksien havainnollistamiseksi on valittu elektronisen sodankäynnin näkökulma, ja tavoitteena on osoittaa älykkäiden antennien tuottama lisäarvo taktisessa radioverkossa. Lisäarvo muodostuu älykkään antennin kyvystä mukauttaa antennin suuntakuvio tietoturvavaatimusten mukaisesti (esimerkiksi mahdollisimman pieni säteilyteho mahdollisen vastustajan suuntaan tai keskinäishäiriön välttäminen omien solmujen kesken). Älyantenneja on tutkittu jo vuosikymmeniä, eikä kognitiivinen prosessi itsessään paranna älykkään antennin ominaisuuksia, mutta kognitiivinen prosessi mahdollistaa esimerkiksi koko radioverkon laajuisen antennien suuntakuvioiden optimoinnin.

Järjestelmien tekninen yhteentoimivuus muodostuu kaikkien tietoliikennejärjestelmän kerrosten yhteensopivuudesta. Kahden eri järjestelmän rajapinnassa molemmissa järjestelmissä on noudatettava esimerkiksi samaa tietoliikenne- ja reititysprotokollaa, aaltomuotoa tai fyysistä liityntää, jotta rajapinta käyttäytyy läpinäkyvästi tietoliikenteen kannalta. Mikäli rajapinnoissa joudutaan käyttämään manuaalista tiedonsiirtoa tai tekemään protokollamuunnoksia, informaatiota voi hävitä tai sen laatu voi heiketä. Yhteentoimivuuden kattava tarkastelu ei laajuudeltaan mahdu tähän tutkimukseen, joten yhteentoimivuutta tarkastellaan analysoimalla verkkosolmujen saavutettavuutta karkealla tasolla. Saavutettavuudella tarkoitetaan solmun kykyä kommunikoida muiden verkon solmujen kanssa. Saavutettavuuden tasoon vaikuttaa yhteydellä olevien rajapintojen määrä. Nykyisissä taktisissa tietoliikenneverkoissa saavutettavuutta heikentää heterogeenisiä teknologioiden käyttö. Nykyiset kenttäradiot, taktiset radiolinkit ja kaupalliset tietoliikennelaitteet eivät kykene kommunikoimaan keskenään läpinäkyvästi. Kognitiivisessa verkossa tietoliikennelaitteet kykenevät vihtamaan tietoa ominaisuuksistaan, jolloin tietoliikenneverkon protokollat ja parametrien arvot voidaan valita optimaalisesti koko verkon näkökulmasta.

Kuten jo aiemmin todettiin, kognitiivinen prosessi ei ole välttämättä ainoa tapa parantaa vertailtavia tietoliikenneverkon ominaisuuksia. Jo nykyisilläkin teknologioilla voidaan parantaa edellä mainittuja ominaisuuksia, mutta automaattinen parametrin säätöprosessi rajoittuu usein vain pieneen osaan tietoliikennejärjestelmää. Automaattisesti voidaan säätää esimerkiksi radiolaitteen lähetystehoa tai modulaatiolajia, mutta vasta kognitiivinen prosessi lisää laitteeseen kyvyn oppia aiemmista tapahtumista. Kognitiivisessa verkossa parametrien havainnointi ei rajoitu pelkästään muutamaan, vaan verkon tilaa havainnoidaan koko verkon laajuisesti ja syntyneen tilannetietoisuuden perusteella verkon resurssit voidaan säätää optimaalisesti ajan, paikan ja vaaditun palvelutason suhteen.

3.2.1 Mukautumisviive

Taktisen tietoliikenneverkon tila on harvoin pitkään stabiili. Taistelutilassa tapahtuvat muutokset ja operaation dynaamisuus muuttavat tietoliikenneverkon vaatimuksia jatkuvasti. Liikkeessä tapahtuva tilannetietoisuuden muodostaminen (sensorit, tiedustelu), johtaminen ja tulenkäyttö vaativat verkon reaaliaikaista mukautumista.

Tietoliikenneverkon mukautumisviiveen laskemiseen ei löydy perusteoriaa. Dynaamisista verkoista löytyy jonkin verran tutkimusta, mutta niissä tutkimuksen kohde on yleensä verkon muutoksista yksittäiseen palveluun aiheutunut viive [25] tai datapaketin siirtämisen viive

[52]. Mukautumisviiveen laskemiseksi tehdään alkuoletus, jonka mukaan mukautumisviive muodostuu neljästä osatekijästä:

- Vaatimuksen muodostaminen ja havaitseminen (τ_{obs})
- Muutosten suunnittelu (τ_{plan})
- Parametrien laskenta (τ_{calc})
- Muutosten toimeenpano (τ_{conf})

Viive τ_{obs} syntyy, kun sovellusten tai käyttäjien tietoliikennepalvelulle asettama uusi vaatimus muodostetaan ja vaatimus havaitaan. Seuraavassa vaiheessa muodostuu viive τ_{plan}, kun vaatimusten perusteella suunnitellaan verkkoon tarvittavat muutokset. Kolmannessa vaiheessa syntyy viive τ_{calc}, kun muutoksiin liittyen lasketaan verkon parametreille (esim. taajuudet, salausavaimet, sijainnit) uudet arvot. Viimeisessä vaiheessa aiheutuu viive τ_{conf}, kun uudet parametriarvot konfiguroidaan järjestelmän solmuihin. Mukautumisesta aiheutuva kokonaisviive voidaan kirjoittaa muodossa

$$\tau_{tot} = \tau_{obs} + \tau_{plan} + \tau_{calc} + \tau_{conf} \,. \tag{7}$$

Monisolmuisessa verkossa viiveen suuruus on verrannollinen muutoksien, muutettavien parametrien ja muutoksia sisältävien solmujen määrään. Nykyisissä järjestelmissä pääosa verkon muutoksista tehdään manuaalisesti.

Taulukossa 2 on esitetty verkkosolmujen määrän vaikutus viiveeseen manuaalisessa ja kognitiivisessa verkossa. Havaintoihin oletetaan molemmissa tapauksissa kuluvan vakioaika ($\Delta t_{obs,M}$ ja $\Delta t_{obs,C}$). Verkon muutosten suunnitteluun, muutosten laskemiseen ja konfigurointiin kuluva aika oletetaan riippuvan solmujen määrästä n. Riippuvuus ei kuitenkaan ole lineaarinen, koska voidaan olettaa, että verkkosolmujen määrän kasvaminen lisää verkon monimutkaisuutta eksponentiaalisesti. Esimerkiksi täysin kytketyn (*engl. fully connected*) verkon solmujen välisten linkkien määrä kasvaa suhteessa solmujen määrän neliöön ($n(n\text{-}1)/2$) [34]. Myös verkkoparametrien optimoinnin edellyttämään iterointilaskentaan kuluva aika on pahimmillaan luokkaa $O(n^2)$ [13]. Potenssivakioilla α, β ja γ pyritään kuvaamaan edellä mainittua ei-lineaarista käytöstä. Vakiot $\Delta t_{plan,M}$ ja $\Delta t_{plan,C}$ kuvaavat yhden solmun muutosten suunniteluun kuluvaa aikavakiota.

Solmun parametrien laskentaviiveen oletetaan molemmissa tapauksissa olevan sama (Δt_{calc}), kun käytetään tietokonepohjaista laskentaa, mutta manuaalisesti ohjelmoitavassa verkossa laskentaparametrien syöttäminen vie ajan A.

Taulukko 2. Solmujen määrän (n) vaikutus mukautumisviiveeseen.

	Manuaalinen	Kognitiivinen
τ_{obs}	$\Delta t_{obs,M}$	$\Delta t_{obs,C}$
τ_{plan}	$\Delta t_{plan,M} n^{\alpha}$	$\Delta t_{plan,C} n^{\alpha}$
τ_{calc}	$A+\Delta t_{calc} n^{\beta}$	$\Delta t_{calc} n^{\beta}$
τ_{conf}	$\Delta t_{conf} n/N$	$\Delta t_{conf} n^{\gamma}$

Konfigurointivaiheessa yhden solmun ohjelmointiin kuluu aika Δt_{conf} . Manuaalisessa verkossa kokonaisviive riippuu suoraan solmujen määrästä n, mutta käytettäessä useaa ohjelmoijaa rinnan konfigurointiin kuluva aika voidaan jakaa ohjelmoijien määrällä N.

3.2.2 Spektrinkäytön tehokkuus

Spektrin hyödyntämisaste määritetään suhteessa käytettyyn taajuuden, geometrisen tilan ja ajan määrään [54]. Spektrinkäyttö voidaan laskea kaavalla

$$U = B \cdot S \cdot T \,, \tag{8}$$

missä U on käytetyn spektritilan koko (Hz·m^3·s). B on spektrin leveys, S geometrinen tila ja T aika. Spektrinkäytön tehokkuus lasketaan siirretyn informaation (M) ja käytetyn spektritilan U suhteena eli

$$U_{eff} = \frac{M}{U} = \frac{M}{B \cdot S \cdot T} \,. \tag{9}$$

Siirretyn informaation suhde aikaan (M/T) on sama kuin järjestelmän kapasiteetti eli tiedonsiirtonopeus R (bit/s), jolloin voidaan kirjoittaa

$$U_{eff} = \frac{R}{B \cdot S} \,. \tag{10}$$

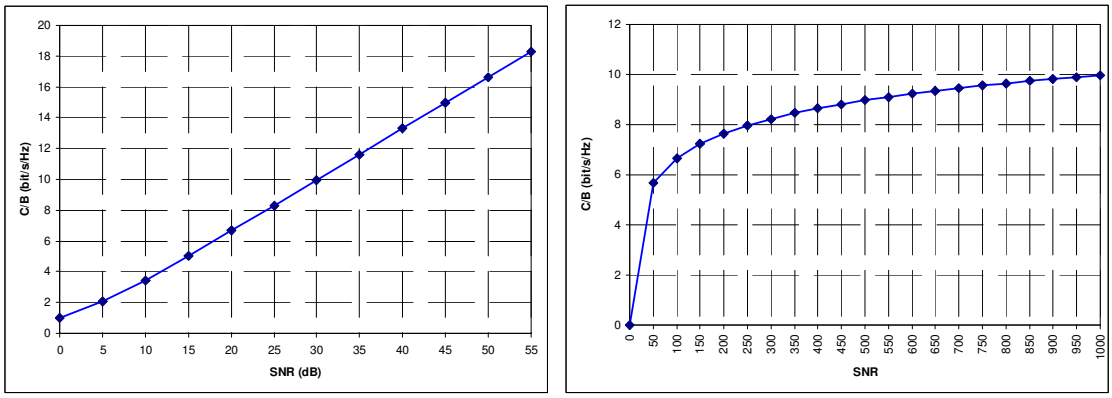
Geometrisen tilan pysyessä vakioina spektrinkäytön tehokkuus riippuu siis käytössä olevasta spektrin leveydestä ja datansiirtonopeudesta. Käytössä olevaa spektrinleveyttä rajoittaa yleensä taajuushallintoviranomaisen (Suomessa Viestintävirasto) antama taajuuslupa tai radiojärjestelmän ominaisuudet. Vaikka taajuuslupa mahdollistaisikin tietyn taajuusalueen käytön, radiojärjestelmät eivät käytännössä mahdollista spektrin käyttöä sataprosenttisesti. Radiokanavat tarvitsevat suojavälin, ja esimerkiksi taktisessa tietoliikenneverkossa yksittäinen radio-

kanava ei ole allokoituna jatkuvasti. Näin spektriin jää väistämättä käyttämättömiä alueita ajan ja paikan suhteen.

Spektrinkäytön tehokkuuteen liittyy keskeisesti radiokanavan tiedonsiirtokapasiteetti. Kapasiteettiin voidaan vaikuttaa usealla eri tekijällä (modulaatio, koodaus, antenniratkaisut jne.), mutta teoreettinen yläraja radiokanavan kapasiteetille määräytyy Shannonin yhtälöstä [41]

$$C = B\log_2(1+\gamma), \tag{11}$$

missä C on kapasiteetti (bit/s). B on kanavan kaistanleveys ja γ on signaali-kohinasuhde, joka voidaan laskea radion lähetystehon P ja kohinatehotiheyden N_0 suhteesta $\gamma = P/N_0B$. Shannonin kapasiteettia on yleensä käytetty datanopeuden ylärajana, jota on lähes mahdoton saavuttaa reaalimaailman järjestelmissä. Tosin käyttämällä radiokanavassa turbokoodausta [19] voidaan päästä hyvin lähelle Shannonin kapasiteettirajaa. Kuvassa 12 on esitetty Shannonin tiedonsiirtokapasiteetti (bit/s/Hz) AWGN-kanavassa (valkoinen kohina, vakio tehotiheys).



(a) (b)

Kuva 12. Tiedonsiirtokapasiteetti AWGN-kanavassa. (a) Signaali-kohinasuhde desibeleissä ja (b) signaali-kohinasuhde normaalina suhdelukuna.

Kuvasta huomataan, että teoreettinen kapasiteetti kasvaa lineaarisesti, kun signaali-kohinasuhde esitetään desibeleissä (a). Mikäli vaaka-asteikolla käytetään signaalitehon ja kohinatehon suhdetta ilman desibelejä, kapasiteetti kasvaa logaritmisesti eli signaali-kohinasuhteen paraneminen ei vaikuta samassa suhteessa kapasiteetin kasvuun (b).

Radiokanavan kapasiteettiin vaikuttaa signaalin modulointitapa. Tietoliikennejärjestelmissä käytetään digitaalisia modulointilajeja, joilla pyritään suureen datanopeuteen ja spektritehokkuuteen sekä pieneen lähetystehon tarpeeseen ja bittivirhesuhteeseen, mutta usein implementoidessa joudutaan tekemään kompromisseja edellä mainittujen vaatimusten osalta [19]. Sig-

naali-kohinasuhteen kasvaessa voidaan käyttää tehokkaampia modulointitekniikoita, kuten esimerkiksi monitasoisia vaihemodulaatiolajeja QAM (Quadrature Amplitude Modulation) ja PSK (Phase Shift Keying). Näiden taajuusrajoitettujen modulaatiolajien kapasiteetti voidaan laskea kaavasta

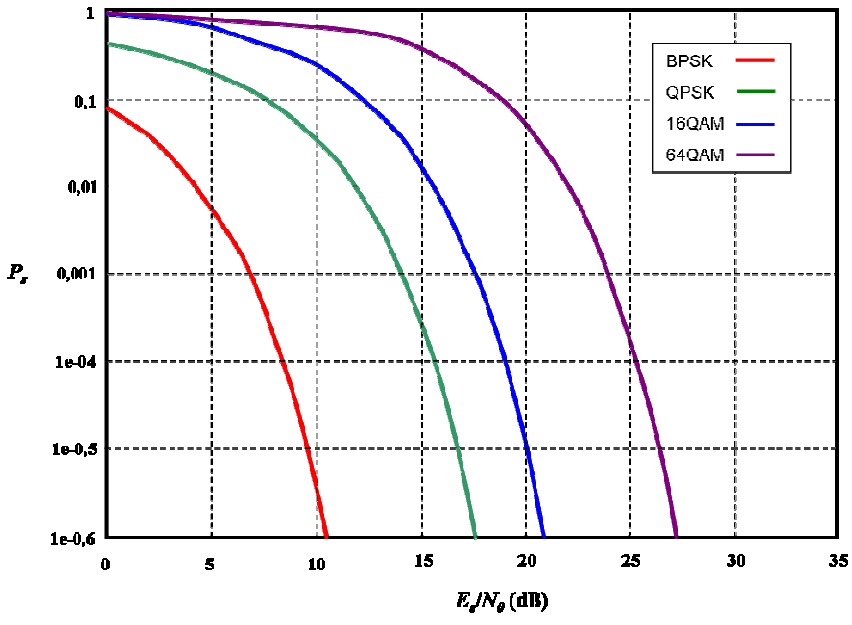
$$R_b/W = \log_2 M, \tag{12}$$

missä M on modulaation symbolien määrä (esim. 16QAM), R_b on bittinopeus, ja W on kaistanleveys. Taulukossa 3 on esitetty eri modulaatiolajien spektritehokkuudet [17].

Taulukko 3. Eri modulaatiolajien teoreettiset spektritehokkuudet.

Modulaatiolaji	Teoreettinen spektritehokkuus
MSK	1 bit/s/Hz
BPSK	1 bit/s/Hz
QPSK	2 bit/s/Hz
8PSK	3 bit/s/Hz
16QAM	4 bit/s/Hz
32QAM	5 bit/s/Hz
64QAM	6 bit/s/Hz
256QAM	8 bit/s/Hz

Monitasoinen modulaatio kasvattaa bittinopeutta, mutta samalla joudutaan kasvattamaan signaali-kohinasuhdetta bittivirhesuhteen minimoimiseksi [38], kuten kuvasta 13 voidaan havaita. Kuvasta voidaan todeta, että bittivirhesuhteen pitämiseksi samana 64QAM-modulaatiossa tarvitaan noin 17 dB parempi signaali-kohinasuhde verrattuna BPSK-modulaatioon.



Kuva 13. Symbolivirhetodennäköisyys (P_s) eri modulaatiolajeilla [55a].

3.2.3 Muokattava antennin suuntakuvio

Älykkäillä antennitekniikoilla voidaan parantaa radioyhteyden laatua minimoimalla monitieetenemisen haittavaikutukset tai toisaalta hyödyntämällä eri teitä edenneet radioaallot. Sotilassovelluksissa älyantennien merkittävä ominaisuus on yleensä sähköisesti muokattava antennin suuntakuvio. Säädettävällä suuntakuviolla voidaan pienentää keskinäishäiriöitä ja ennen kaikkea estää vastustajaa tiedustelemasta radiolähetteitä ja käyttämästä elektronista häirintää. Älyantennin muita hyötyjä ovat:

- kasvanut kantama ja peitto
- pienempi tehon tarve
- parantunut linkin laatu ja kestävyys
- kasvanut spektritehokkuus. [14]

Elektronisen tiedustelun ja häirinnän kannalta tärkeä antennin ominaisuus on antennin suuntaavuus, jolla tarkoitetaan antennin kykyä keskittää säteily haluttuun suuntaan [29]. Suuntaavuus D määritellään suunnan $\mathbf{u}_r$ funktiona [29]:

$$D(\mathbf{u}_r) = 4\pi \frac{W(\mathbf{u}_r)}{P_r}. \tag{13}$$

Kaavassa $W(\mathbf{u}_r)$ on antennin suuntaan $\mathbf{u}_r$ säteilemä tehotiheys avaruuskulmaa kohti, ja P_r on antennin säteilemä kokonaisteho. Antennin vahvistus on muuten sama suure kuin suuntaavuus, mutta antennin säteilytehon sijasta kaavassa (13) on antenniin syötetty teho. Vahvistus on käytännössä suuntaavuutta pienempi, koska osa tehosta kuluu antennin häviöihin [29]. Jos antennin tehohyötysuhteeksi η määritellään antennin säteilytehon ja syötetyn tehon suhde, saadaan antennin vahvistukseksi $G = \eta D$.

Perinteisissä sotilaallisissa radiojärjestelmissä yleisin antennityyppi on ollut ympärisäteilevä monopoliantenni, joka on yksinkertaisesti käytettävissä kannettavissa ja ajoneuvoasenteisissa kenttäradiossa. Monopoliantennissa johtava taso toimii antennin toisena elementtinä, ja pystyyn tästä tasosta eristetty metallilanka toimii säteilevänä elementtinä. Monopoliantenni säteilee vain tason yläpuolelle puoliavaruuteen, joten samaa tehoa käyttämällä sillä saadaan kaksinkertainen tehotiheys verrattuna dipoliantenniin [22]. Toisin sanoen monopoliantennin suuntaavuus on kaksinkertainen. Taistelukentällä maataso on harvoin ideaalinen, jolloin mo-

nopoliantennin vahvistus jää alle teoreettisen. Taulukkoon 4 on listattu yleisimpien monopoli- ja dipoliantennien suuntaavuus.

Taulukko 4. Eri antennityyppien suuntaavuus [22].

Antennityyppi	Suuntaavuus	Suuntaavuus (dBi)
λ/2-dipoli	1,64	2,15
λ-dipoli	2,4	3,8
λ/4-monopoli	3,28	5,15
λ/2-monopoli	4,8	6,8

Älyantennissa antennin suuntakuvion muokkaaminen perustuu joukkoon samanlaisia antennielementtejä. Antennielementit voivat olla yksinkertaisia, koska antenniryhmän säteilyominaisuudet perustuvat elementtien suureen määrään. Muuttamalla antennielementtien vaiheistusta voidaan säteilykeilaa kääntää sähköisesti. Verrattuna yksittäiseen antennielementtiin, joista ryhmä on muodostettu, ryhmällä voidaan saavuttaa suurempi vahvistus ja haluttu suuntakuvio. Ryhmän suuntakuvio on antennielementin suuntakuvion ja ryhmäkertoimen tulo [28]. Ryhmäkerroin on antennielementtien paikan funktio ja se voidaan kirjoittaa [28]

$$f(\mathbf{u}_r) = \sum_{i=1}^{N} e^{jkr_i \cos\alpha_i} \ , \tag{14}$$

missä α_i on elementin paikkavektorin r_i ja säteilysuunnan $\mathbf{u}_r$ välinen kulma ja N on elementtien lukumäärä. Kun antenniryhmän elementtien väli d on pieni aallonpituuteen verrattuna ($d < \lambda$), tasossa olevalle M-elementtiselle antenniryhmälle voidaan laskea suuntaavuus karkeasti kaavalla [55]

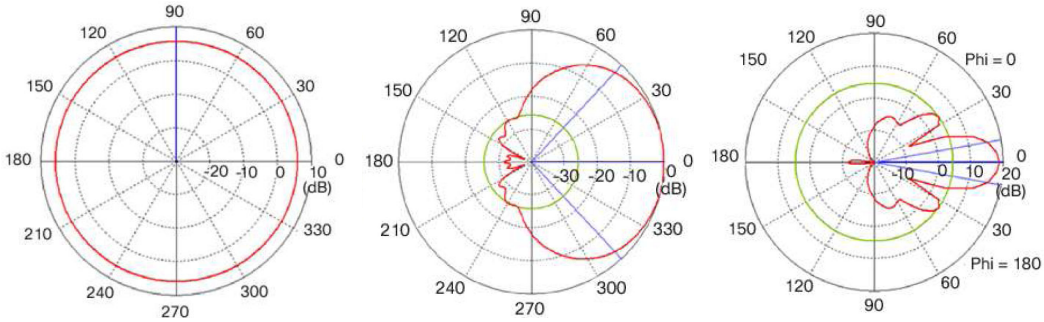
$$D = 2M\frac{d}{\lambda}, \tag{15}$$

Elementtien välin ollessa esimerkiksi $1/10\lambda$ suuntaavuus 10-elemettisellä antenniryhmällä on 2 eli noin 3 dBi. Elementtimäärää lisäämällä voidaan kasvattaa antenniryhmän suuntaavuutta.

Vaiheohjatussa antenniryhmässä jokaisen antennielementin syöttövirtojen vaihetta säädetään erikseen, jolloin antennin nollakohtien (pieni vahvistus) ja maksimien (suuri vahvistus) kulmasijainti muuttuu. N-elementtinen antenniryhmä voi muodostaa N kpl nollakohtia, joilla voidaan merkittävästi vähentää N erillisen häiriölähteen vaikutusta. Mikäli häiriölähteitä on $N_i < N$, häiriölähteet voidaan minimoida, ja lisäksi loput $N - N_i$ antennielementtiä voidaan käyt-

tää diversiteettivahvistuksen synnyttämiseen. Huomioitavaa on, että antenniryhmän on tunnettava häiriölähteiden kulmasijainnit, jotta nollakohdat voidaan suunnata oikein.[19]

Antennien suuntakuvioita on havainnollistettu kuvassa 14. Kuvassa on esitetty monopoliantennin, sektoriantennin ja antenniryhmän suuntakuviot horisontaalisessa tasossa.



(a) (b) (c)

Kuva 14. Antennien suuntakuvioita [6]. (a) Ympärisäteilevä monopoliantenni, (b) sektoriantenni (dipoliryhmä) ja (c) 4 x 4-elementtinen tasoantenniryhmä.

3.2.4 Saavutettavuus

Saavutettavuus kuvaa yksittäisen tietoliikenneverkon solmun kykyä muodostaa yhteys toiseen solmuun [20]. Kuvan 11 mukaisessa verkossa kahden solmun välinen yhteys voi muodostua usean aliverkon ja yhdyskäytävän kautta. Käytössä olevissa taktisissa tietoliikenneverkoissa yhteys voi muodostua automaattisesti, mutta usein vaaditaan ihmistä huolehtimaan yhteyden kytkemisestä rajapinnoissa ja yhdyskäytävissä. Pahimmillaan ihminen voi joutua välittämään manuaalisesti informaatiota aliverkkojen välillä (esimerkiksi yhteensopimaton puheyhteys).

Esimerkiksi koodausmuutosten tai tiedon pakkaamisen vuoksi yhdyskäytävässä voi aiheutua informaation laadun heikkenemistä. Tämän vuoksi saavutettavuutta määriteltäessä on mielekästä tarkastella suorien ja epäsuorien tietoliikennelinkkien määrää verkon solmujen välillä. Linkkien vaikutus voidaan huomioida määrittelemällä saavutettavuudelle muuttuja R_{ij}, joka on solmujen i ja j välisellä yhteydellä olevien, manuaalisia yhdyskäytäviä sisältävien aliverkkojen lukumäärän d_{ij} käänteisluku. Saavutettavuus voidaan määritellä [20]

$$R_{ij} = \frac{1}{d_{ij}}. \tag{16}$$

Termin d_{ij} määrittelyn vuoksi sen oletetaan olevan yksi tai suurempi, mikä tarkoittaa, että saavutettavuuden R_{ij} arvo on 0 (ääretön etäisyys tai ei linkkiä ollenkaan solmujen *i* ja *j* välillä) ja 1 (solmut *i* ja *j* ovat samassa aliverkossa) välillä. Taktisen verkon mallin (kuva 11) mukaisesti tarkasteltavana kohteena on yhtymä (prikaati), jolloin voidaan laskea saavutettavuutta esimerkiksi ryhmätasolta prikaatin esikuntaan tai kahden eri puolilla olevan pataljoonan ryhmien välillä. Saavutettavuutta on järkevää tarkastella koko yhtymän verkon kannalta [20]. Yksittäisen solmun *j* saavutettavuus lasketaan verkon muista solmuista *i* laskettujen saavutettavuuksien R_{ij} keskiarvona

$$R_j = \frac{1}{n}\sum_i R_{ij}\ , \tag{17}$$

missä *n* on verkon solmujen kokonaismäärä. Nykyisten taktisten verkkojen hierarkisuuden vuoksi jokaisen tason aliverkon jäsenellä on yhtä pitkä etäisyys esimerkiksi prikaatin esikuntaan tai komentajaan, jolloin edellä oleva kaava voidaan yksinkertaistaa muotoon

$$R_j = \sum_{all\ i\ in\ s} \frac{1}{d_{ij}} = \sum_{all\ i\ in\ s} \frac{1}{d_{sj}} = \frac{n_s}{d_{sj}}\ , \tag{18}$$

missä d_{sj} on manuaalisia yhdyskäytäviä sisältävien aliverkkojen lukumäärä muodostettaessa yhteys aliverkon *s* solmusta solmuun *j*. Muuttuja n_s on solmujen määrä aliverkossa *s*. Solmun *j* saavutettavuus saadaan laskemalla lopuksi yhteen kaikkien aliverkkojen saavutettavuus:

$$R_j = \frac{1}{n}\sum_s R_{sj} = \frac{1}{n}\sum_s \frac{n_s}{d_{sj}} = \sum \frac{n_s}{n}\frac{1}{d_{sj}} = \sum \omega_s \frac{1}{d_{sj}}\ . \tag{19}$$

Muuttuja ω_s on aliverkossa s olevien solmujen määrän suhde koko verkon solmujen määrään. Solmun *j* saavutettavuusparametri R_j vaihtelee välillä 0 (ei yhteyttä solmuun *j*) ja 1 (kaikki solmut ovat suoraan yhdistetty solmuun *j* eli solmut ovat samassa aliverkossa).

3.3 Analyysin tuloksia

Tarkan mukautumisviiveen laskeminen on haasteellista sekä nykyisissä taktisissa tietoliikenneverkoissa että kognitiivisessa verkossa. Viiveeseen vaikuttavat verkon monimutkaisuus, säädettävien parametrien määrä sekä haluttu verkon tavoitetila. Manuaalista suunnittelua ja konfigurointia vaativassa järjestelmässä ihmisestä johtuvan viiveen yksikäsitteinen määrittäminen voi olla jopa mahdotonta. Empiiristä tutkimustietoa käytössä olevan taktisen tietolii-

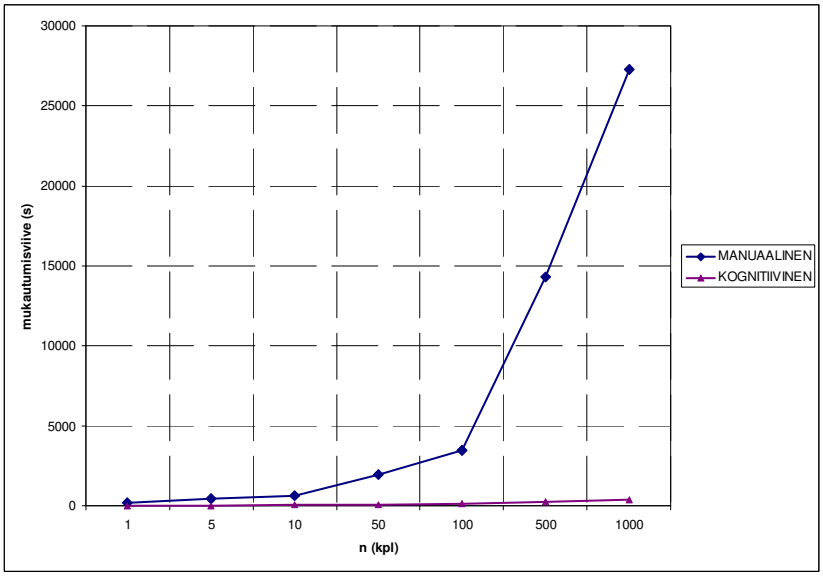
kenneverkon muutoksiin kuluvista aikaviiveistä ei löytynyt, joten tässä analyysissa päädyttiin määrittämään vain suuruusluokaltaan oikeansuuntaiset viiveet. Samalla tavoin pyrittiin määrittämään kognitiivisen verkon mukautumisviiveet oikeaan suuruusluokkaan, kun lähtökohtana on automaattisesti tietokoneiden avulla tapahtuva laskenta ja verkon konfigurointi.

Taulukko 5. Mukautumisviiveen laskennassa käytetyt arvot.

	Manuaalinen	Kognitiivinen
Δt_{obs}	10000 ms	1000 ms
Δt_{plan}	100000 ms	5000 ms
Δt_{calc}	1000 ms	1000 ms
Δt_{conf}	120000 ms	5000 ms
A	60000 ms	-
N	5	-
α, β, γ	0,5	0,5

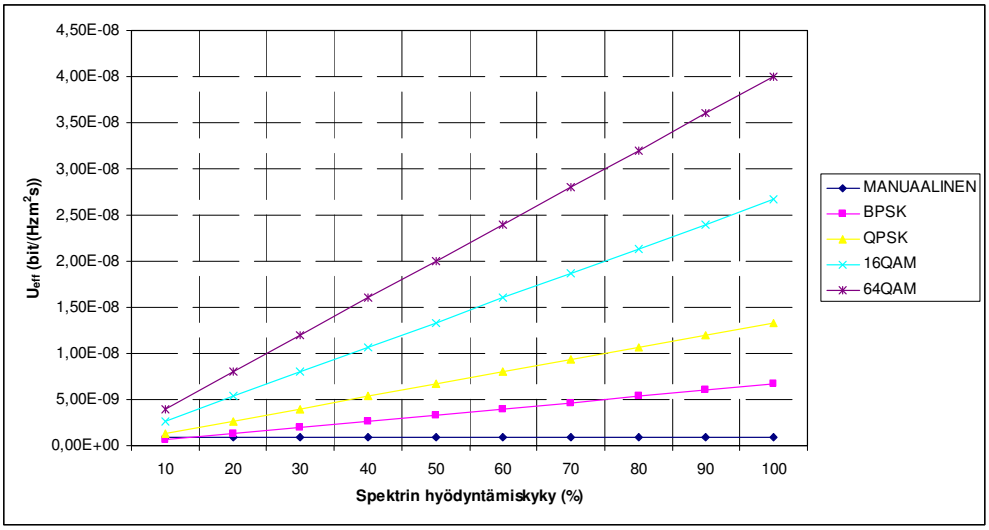
Taulukossa 5 on mukautumisviiveen laskennassa käytettyjen parametrien arvot. Arvot eivät perustu empiirisiin kokeisiin tai teoreettiseen laskentaan, vaan perustuvat tutkijan omaan päättelyyn manuaalisen ja tietokoneen tekemään laskentaan tai suunnitteluun kuluvan ajan erosta. Huomioitavaa on, että annetut viiveet ovat korkeintaan suuntaa antavia. Peruslähtökohta on, että tietokoneen tekemään laskentaa kuluva aika on tyypillisesti sekuntiluokkaa, kun taas ihmisen suorittama laskenta tai suunnittelu vie aikaa kymmeniä sekunteja.

Kuvassa 15 on esitetty taulukon 4 arvoilla laskettu mukautumisviive solmujen määrän funktiona käyttäen kaavaa (7). Solmujen määrän kasvaessa manuaalisesti toteutettava verkonhallinta (muutosten tekeminen) vie aikaa huomattavasti enemmän kuin kognitiivinen, automaattisesti muutoksia tekevä järjestelmä. Kuvasta 15 voidaan nähdä, että luvussa 3.2.1 esitetyn mallin mukaan laskettu mukautumisviive kasvaa manuaalisessa järjestelmässä expotentiaalisesti. Automaattisessa ja itsenäiseen päätöksentekoon pystyvässä kognitiivisessa järjestelmässä mukautumisviive näyttää kasvavan lähes lineaarisesti. Muistettava on, että esimerkiksi rinnakkaisten operaattorien määrää tai potenssivakioiden arvoja muuttamalla mukautumisviiveen käyttäytyminen muuttuu ja järjestelmien välinen ero ei välttämättä ole näin huomattava.



Kuva 15. Mukautumisviive solmujen määrän funktiona.

Spektrinkäytön tehokkuutta on tarkasteltu määrittelemällä taktiselle tietoliikenneverkolle maantieteellinen alue (S = 150 km^2), jonka koko vastaa maavoimien yhtymän tyypillistä toiminta-aluetta. Käytössä oleva kaistanleveys (B = 20 MHz) on tässä tarkastelussa yhtymän VHF-kenttäradioille allokoitu kokonaistaajuuskaista, kun huomioidaan VHF-radioiden teknineen suorituskyky ja vierekkäisten yhtymien tarvitsemat taajuuksien suojavälit. Kuvassa 16 on esitetty spektrinkäytön tehokkuus (kaava 10) eri modulaatiolajeilla spektrin hyödyntämiskyvyn funktiona. Spektrin hyödyntämiskyvyllä tarkoitetaan radiojärjestelmän kykyä käyttää järjestelmälle allokoitua taajuuskaistaa tilan ja ajan suhteen. Nykyisessä kenttäradiojärjestelmässä hyödyntämiskyky on sama kuin yhtäaikaisten radioyhteyksien määrä. Tässä analyysissä oletetaan, että nykyisessä kenttäradioverkossa jokaiselle aliverkolle voidaan varata kolme liikennöintikanavaa, jolloin kuvan 11 mukaisessa verkossa liikennöintikanavien määrä yhtymän alueella on yhteensä 3 x 39 = 117 kappaletta.

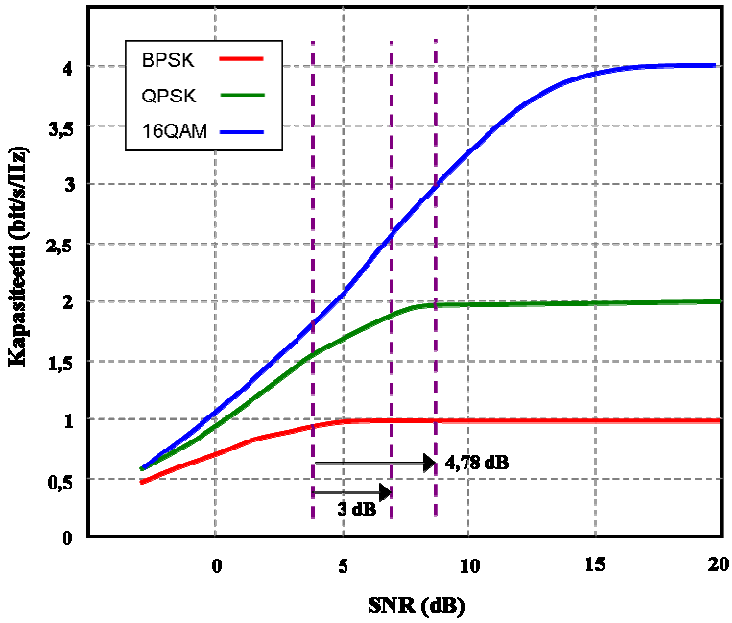


Kuva 16. Spektrinkäytön tehokkuus hyödyntämiskyvyn funktiona.

Yksittäisen radiolähetteen kaistanleveytenä on molemmissa verkkotyypeissä (manuaalinen ja kognitiivinen) nykyisten kenttäradioiden käyttämä kanavaleveys 25 kHz. Digitaaliset kenttäradiot käyttävät BPSK-modulaatiota. Kognitiivinen radiojärjestelmä voi lisäksi käyttää QPSK-, 16QAM- ja 64QAM-modulaatioita tilanteen mukaan. Eri modulaatioilla saavutettu teoreettinen tiedonsiirtonopeus on laskettu kaavalla (12). Laskennassa ei ole huomioitu yhtymän toiminta-alueella (S = 150 km^2) tapahtuvaa taajuuksien uusiokäyttöä, mikä parantaisi merkittävästi spektrinkäytön tehokkuutta nykyjärjestelmässä. Taajuuksien uudelleenkäyttö on mahdollista toteuttaa esimerkiksi älykkäitä antenneja ja signaalikoodausta käyttämällä.

Spektrinkäytön tehokkuuden analysoimisessa on pyritty osoittamaan, kuinka tiedonsiirtokapasiteettia voidaan kasvattaa järjestelmällä, joka kykenee hyödyntämään tehokkaampia modulaatiomenetelmiä ja käyttämään koko käytettävissä olevan taajuuskaistan tehokkaasti. Modulaatiomenetelmien mukautuva käyttö ei ole kognitiivisen verkon erityisominaisuus, vaan ominaisuus on käytössä nykyään erilaisissa radiojärjestelmissä (esimerkiksi WiMAX-standardi [36]). Merkityksellisempää on kognitiivisen verkon kyky käyttää ominaisuutta koko verkonlaajuisen tilannetietoisuuden perusteella. Modulaatiolajin valinta ei perustu pelkästään radiokanavan ominaisuuksien tarkkailuun, vaan siihen vaikuttavat parhaimmillaan koko verkon tilatieto ja ennen kaikkea aiemmin opittu käyttäytyminen. Vapaiden taajuuskaistojen tehokas käyttö edellyttää kykyä tarkkailla spektriä ja kykyä tehdä nopeita päätöksiä taajuuksien käytöstä. Tähän toiminnallisuuteen nykyiset taktiset tietoliikennejärjestelmät eivät pysty.

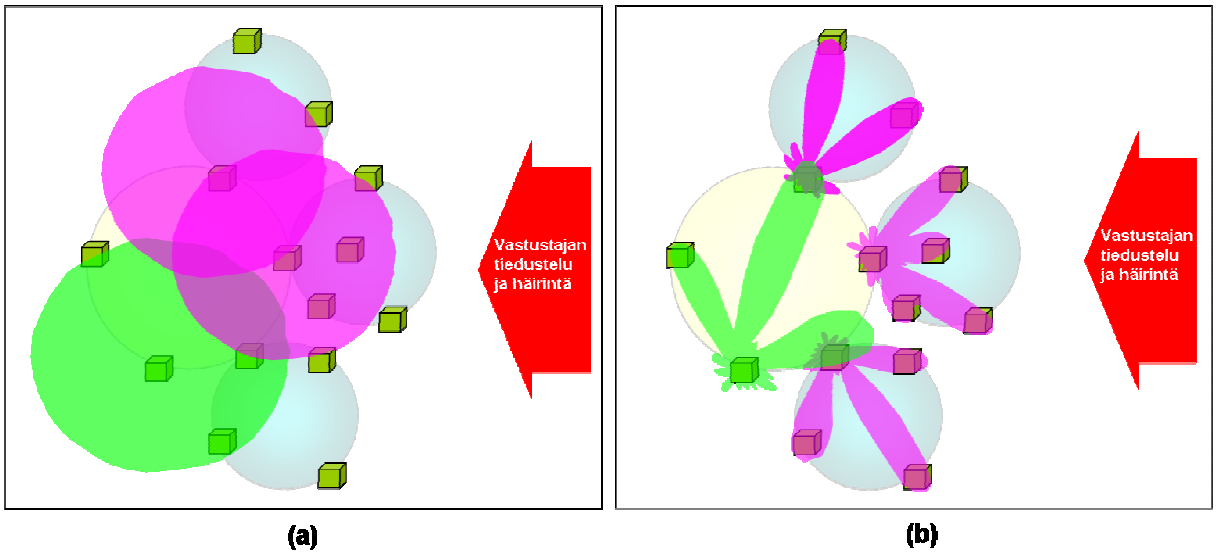
Antennin suuntakuvion muokattavuuden hyötyjä tarkastellaan tiedonsiirtonopeuden ja elektronisen tiedustelun kannalta. Kuvassa 17 on esitetty kaksi- ja kolmielementtisen antenniryhmän vaikutus tiedonsiirtonopeuteen eri modulaatiolajeilla. Kuvan tilanteessa ilman antenniryhmää (yksi elementti) signaali-kohinasuhteen oletetaan olevan 4 dB, jolloin esimerkiksi 16QAM-modulatiolla päästään kapasiteettiin 1,8 bit/s/Hz. Ideaalisessa tilanteessa yhden elementin lisääminen parantaa antennivahvistuksen kaksinkertaiseksi (SNR = 7 dB), jolloin saavutetaan kapasiteetti noin 2,6 bit/s/Hz. Teoreettinen tiedonsiirtonopeuden parannus on näin noin 44 %. Kolmannen elementin lisääminen kasvattaa ideaalitilanteessa vahvistuksen kolminkertaiseksi, jolloin vahvistus kasvaa 4,78 dB ja 16QAM:n tapauksessa kapasiteetti kasvaa arvoon 3,0 bit/sHz eli lisäys on noin 67 %. Mikäli SNR on alun perin jo suuri (yli 15 dB), antennivahvistuksen kasvattaminen ei lisää kanavakapasiteettia.



Kuva 17. Antenniryhmän vaikutus kanavakapasiteettiin eri modulaatiolajeilla. Kuvan pohjautuu viitteessä [38] esitettyihin arvoihin.

Kuvassa 18 on havainnollistettu ympärisäteilevien ja älykkäiden antennien käyttöä taktisessa radioverkossa. Ympärisäteilevä antenni on käytännössä ainoa antennityyppi, joka mahdollistaa nykyjärjestelmissä yhteyksien muodostamisen liikkeessä. Ympärisäteilevää antennia käytettäessä (kuva 18a) radiosignaalin tehoa ei voida suunnata haluttuun suuntaan, vaan teho leviää horisontaalisessa tasossa joka suuntaan. Yhteysetäisyyden kasvaessa tehoa joudutaan lisäämään suhteessa merkittävästi enemmän kuin suuntaavaa antennia käytettäessä. Tehoa lisättäessä aiheutetaan mahdollisesti keskinäishäiriöitä sekä kasvatetaan samalla tehotasoa vastustajan suuntaan.

Älyantenneja käytettäessä (kuva 18b) suuntakuviota voidaan säädellä taistelukentän vaatimusten mukaan optimaaliseksi. Solmun (ajoneuvon) ollessa liikkeessä suuntakuviota voidaan säätää siten, että antennin suuntakuvion maksimi on aina kohti vastaanotinta. Teoreettisesti sivukeilat voidaan poistaa kokonaan, mutta nykytekniikalla toteutetuissa ja käyttökelpoisissa antenniratkaisuissa sivukeilojen vahvistus voi olla jopa 30 dB pienempi kuin pääkeilan [16]. Noin 30 db vaimennus vastaa karkeasti tiedusteluetäisyyden pienentymistä esimerkiksi 50 km:stä noin 10 km:iin, kun lähetteen taajuus on 50 MHz, lähetys- ja vastaanottoantennien korkeudet ovat 1 m ja 10 m ja laskennassa käytetään Eglin mallia [27].



Kuva 18. Ympärisäteilevillä (a) ja älykkäillä antenneilla varustetun radioverkon antennien suuntakuvion havainnollistaminen.

Yksittäisen älyantennin toteuttaminen ei vaadi kognitiivista toiminnallisuutta, mutta kognitiivisessa radiojärjestelmässä älyantennien ominaisuuksia voidaan hyödyntää optimaalisesti. Antennin suuntakuvion mukauttaminen ei perustu yksittäisen solmun toimintaan, vaan suuntakuviot muodostetaan tilanteeseen ja vastustajaan nähden optimaalisesti.

Taulukossa 6 on laskettu nykyisen järjestelmän saavutettavuutta kuvan 11 tietoliikenneverkossa. Laskennassa oletetaan, että jokaisen aliverkon välillä on yhdyskäytävä, joka aiheuttaa tietoliikenneyhteyden laadun heikkenemistä. Taulukossa tarkastellaan saavutettavuutta prikaatin esikunnan (R_j) suhteen. Taulukon riveillä on laskettu saavutettavuus jokaiselta verkon tasolta käyttäen kaavoja (18) ja (19).

Taulukko 6. Saavutettavuus (prikaatin esikunta) nykyisessä taktisessa tietoliikenneverkossa.

	n_s	ω_s	d_{sj}	ω_s/d_{sj}
joukkue	81	0,60	4	0,15
komppania	36	0,267	3	0,089
pataljoona	12	0,089	2	0,044
prikaati	6	0,044	1	0,044
YHTEENSÄ	135			**0,328**

Kognitiivisessa verkossa informaation laatua heikentäviä yhdyskäytäviä on vähän tai ei ollenkaan. Taulukkoon 7 on laskettu saavutettavuus tilanteessa, jossa kognitiivisella verkkoinfrastruktuurilla vähennetään yhdyskäytävien määrää merkittävästi. Tilanteessa oletetaan, että ainoat yhdyskäytävät muodostuvat pataljoonaverkkojen ja prikaativerkon välille. Yhteys pa-

taljoonista tai sen alemmilta tasoilta prikaatin esikuntaan muodostuu yhden yhdyskäytävän kautta (kaksi aliverkkoa).

Taulukko 7. Saavutettavuus (prikaatin esikunta) nykyisessä taktisessa tietoliikenneverkossa.

	n_s	ω_s	d_{sj}	ω_s/d_{sj}
joukkue	81	0,60	2	0,30
komppania	36	0,267	2	0,133
pataljoona	12	0,089	2	0,044
prikaati	6	0,044	1	0,044
YHTEENSÄ	135			**0,522**

Taulukoista voidaan nähdä, että saavutettavuus kasvaa kymmeniä prosentteja, kun peräkkäisten yhdyskäytävien määrä prikaatissa vähenee. Käyttämällä saman valmistajan laitteita ja yleisiä standardeja rajapintojen häiriötekijöitä voidaan poistaa jo nykyisissä järjestelmissä. Esimerkiksi ad hoc -tekniikat [31] mahdollistavat radioverkkojen joustavan muodostumisen eri toimijoiden kesken. Verkon topologia on mielivaltainen ja voi muuttua ennustamattomasti. Teoriassa ad hoc -tekniikalla voidaan toteuttaa koko prikaatin tietoliikenneverkko, jolloin kaikki solmut pystyvät kommunikoimaan toistensa kanssa ilman yhdyskäytäviä. Ad hoc -toiminallisuus rajoittuu kuitenkin vain tiettyihin järjestelmiin ja ennalta määrättyyn verkonmuodostustapaan. Kognitiivinen verkko kykenee paremmin hyödyntämään heterogeenistä tietoliikenneinfrastruktuuria ja erityyppisiä teknologioita, jolloin ad hoc -toiminnallisuus on koko verkon laajuista käyttäytymistä.

3.4 Johtopäätökset

Työn toisen osan tavoitteena oli esimerkkiominaisuuksien avulla havainnollistaa kognitiivisen tietoliikenneverkon vaikutuksia nykyisiin taktisiin verkkoihin. Tarkastelun kohteena oli langaton taktinen tietoliikenneverkko, joka nykyään muodostuu pääosin erilaisista radiojärjestelmistä. Analyysin kohteeksi valittiin neljä tietoliikenneverkon ominaisuutta, joita tutkittiin sekä nykyjärjestelmän että kognitiivisen verkon näkökulmasta. Tavoitteena ei ollut laskea absoluuttista suorituskykyä näiden ominaisuuksien suhteen, vaan paremminkin karkealla tasolla osoittaa, millaista lisäarvoa kognitiivinen toiminnallisuus tuo verkostopuolustuksen taktiselle tasolle. Työn laajuuden vuoksi ominaisuuksia käsiteltiin pelkistetyin esimerkein. Tutkittavat ominaisuudet valittiin ensimmäisen osan johtopäätösten perusteella. Tietoliikenneverkon kokonaissuorituskyvyn laskeminen olisi ollut liian monimutkainen ja laaja tehtävä tämän tutkimuksen kannalta, joten työssä päädyttiin ainoastaan havainnollistamaan mahdollista suorituskyvyn paranemista yksittäisten ominaisuuksien perusteella.

Tietoliikenneverkon mukautumisviive on luonnollisesti suurempi manuaalisesti operoitavassa kuin automaattisesti toimivassa verkossa. Poistamalla verkosta manuaaliset prosessin vaiheet verkon mukautumisnopeus kasvaa merkittävästi. Manuaalisesti hallittavassa verkossa mukautumisviive kasvaa jyrkästi solmujen määrän kasvaessa. Kognitiivisessa verkossa viivettä rajoittaa tietokoneiden laskentakapasiteetti ja konfigurointiin kuluva aika. Mukautumisviiveen vertailu tehtiin erittäin karkeilla lähtöarvoilla tutkitun tiedon puutumisen vuoksi. Lisäksi mukautumisviiveen laskentaan käytetty kaava pohjautui tutkijan omaan kokemukseen tietoliikenneverkkojen suunnittelusta ja konfiguroinnista, joten tulosten luotettavuuteen on suhtauduttava riittävän kriittisesti.

Spektrinkäytön tehokkuus on kognitiivisen radioverkon merkittävin ominaisuus. Nykyiset taktiset radiojärjestelmät kykenevät hyödyntämään vain pienen osan prikaatilla käytössä olevista taajuuksista. Paremmalla taajuusallokoinnilla ja tehokkaiden modulaatiomenetelmien käytöllä radioverkon tiedonsiirtokapasiteetti voidaan kasvattaa moninkertaiseksi. Kognitiivinen verkko mahdollistaa modulaatiomenetelmien joustavan käytön ja vapaiden taajuuksien tehokkaan hyödyntämisen ajan ja paikan suhteen. Lisäksi kognitiivinen prosessi pystyy hyödyntämään älykkäiden antennien suorituskyvyn koko verkon kannalta optimaalisesti. Myös solmujen saavutettavuus paranee kognitiivisessa verkossa. Nykyjärjestelmissä verkkojen välillä voi olla useita yhdyskäytäviä ja joihinkin solmuihin ei ole saavutettavuutta ollenkaan. Yhteisiä teknologioita ja standardeja käyttämällä yhdyskäytävien määrää voidaan pienentää, mutta ideaalinen kognitiivinen verkko mahdollistaa koko verkonlaajuisen saumattoman kommunikoinnin.

Vertailun tulokset osoittavat, että älykkyyttä lisäämällä tietoliikenneverkon ominaisuuksia voidaan käyttää joustavammin ja tehokkaammin. Kognitiivisen prosessin käyttö edellyttää kuitenkin ohjelmallisesti muokattavan tietoliikennejärjestelmän rakentamista. Järjestelmän parametrien arvoja on pystyttävä muokkaamaan päätöksenteon mukaisesti. Ohjelmoitavan tietoliikennejärjestelmän rakentaminen on osoittautunut haasteelliseksi, kuten ohjelmistoradion kehittäminen on osoittanut. Taktisella tasolla vaatimuksena on usein kannettava ja vähän virtaa kuluttava radiolaite. Vaatimus on erittäin haastava, koska laitteelta vaaditaan samaan aikaan suurta laskentakapasiteettia ja ohjelmoitavuutta, mikä kuluttaa runsaasti energiaa.

Nykyisen taktisen verkon ja kognitiivisen verkon ominaisuuksien vertailulla pyrittiin ensisijaisesti havainnollistamaan kognitiivisen toiminnallisuuden luomia mahdollisuuksia. Valittujen ominaisuuksien analysointi toimii hyvänä lähtökohtana tarkemmalle ja laajemmalle jatko-

tutkimukselle, jonka perusta voisi muodostua tilannetietoisuuden ja päätöksenteon mekanismien kehittämisestä ja implementoinnista.

4 YHDISTELMÄ

Tutkimuksen ensimmäisenä tavoitteena oli selvittää paradigmatutkimuksen avulla kognitiivisten verkkojen soveltuvuutta verkostopuolustuksen konseptiin. Päämääränä oli selvittää tiedon jakamisen vaatimuksia verkostopuolustuksessa sekä kuvata kognitiivisen verkon konsepti ja perusominaisuudet, ja näin tuottaa synteesi kognitiivisten verkkojen hyödyistä verkostopuolustuksessa. Tutkimuksen toisena tavoitteena oli vertailla nykyistä taktisen tietoliikenneverkon ja kognitiivisen verkon teknistä suorituskykyä neljän verkon ominaisuuden avulla, ja näin osoittaa kognitiivisen verkon tuottama lisäarvo taktiseen tietoliikennejärjestelmään. Vertailua varten luotiin yksinkertainen taktisen verkon malli ja määritettiin vertailtavat ominaisuudet. Tutkimuksessa ei tarkasteltu kognitiivisten verkkojen aiheuttamaa mahdollista suorituskyvyn heikkenemistä.

Verkostokeskeinen sodankäynti on informaatioylivoiman mahdollistava toimintakonsepti, jonka teorian mukaan sotilaallisen joukon taisteluvoimaa voidaan kasvattaa verkottumisen avulla. Verkottuminen ei ole vain teknistä, vaan taistelukentän toimijat verkottuvat myös prosessien, toiminnan ja informaation jakamisen näkökulmasta. Tietoliikennejärjestelmää tarvitaan informaation nopeaan, turvalliseen ja oikea-aikaiseen jakamiseen päätöksenteon laadun parantamiseksi sekä vaikuttavien elementtien ohjaamiseksi. Puolustusvoimissa ei ole tällä hetkellä vahvistettua doktriinia verkostopuolustuksesta, mutta puolustusministeriön tietohallintostrategiassa verkostopuolustus on määritelty kaikkien kokonaismaanpuolustuksen toimijoiden verkottamiseksi yhteisten prosessien, toimintatapojen ja integroitujen tietoverkkojen kautta. Merkittävä ero yhdysvaltalaiseen paradigmaan on ollut verkostopuolustuksen toimijoiden määritteleminen kattamaan kaikki yhteiskunnan elintärkeiden toimintojen rakentamisessa ja ylläpidossa tarvittavat yhteisöt.

Verkostopuolustusta tukevan tietoliikennejärjestelmän rakentaminen on vaativaa. Erityyppisten toimijoiden (viranomaiset, kumppanit, järjestöt) tietotekninen verkottaminen luotettavasti ja turvallisesti on haastavaa, koska verkkojen yhdistäminen lisää yleensä myös tietoturvariskien määrää. Verkottuminen ulottuu myös sodankäynnin taktiselle tasolle, jossa kiinteiden tietoliikennejärjestelmien sijaan käytetään liikkuvia, yleensä langattomia tietoliikenneverkkoja. Taktisella tasolla tilanteet muuttuvat nopeasti, jolloin tietoliikenneverkoilla pitäisi olla kyky nopeaan mukautumiseen ja uusien yhteyksien muodostamiseen. Verkostopuolustuksessa tär-

keimpiä vaatimuksia tietoliikenneverkolle ovat yhteydellisyys, verkkosolmujen liityntävalmius ja verkon hallittavuus.

Kognitiiviset verkot ovat mielenkiintoinen tutkimusala verkostopuolustuksen näkökulmasta. Kognitiivinen verkon paradigma ei määrittele uusia verkon ominaisuuksia eri verkkokerroksille, vaan paremminkin lisää kognitiivisen prosessin verkon kaikkiin verkon solmuihin ja kerroksiin. Kognitiivinen verkko mahdollistaa verkon automaattisen mukautumisen ilman manuaalista operaattoria. Tietoliikennejärjestelmä kykenee näin tuottamaan tarvittavat tiedonsiirtopalvelut katkotta tai lähes katkotta taistelukentän tilanteiden vaihdellessa. Paradigmatasolla kognitiivisten verkkojen käytöstä löydettiin neljä tietoliikennejärjestelmän suorituskykyä parantavaa tekijää: aika, tietoturva, resurssien tehokkaampi käyttö ja yhteentoimivuus.

Kognitiivinen, automaattisesti mukautuva verkko kykenee vastaamaan nopeasti verkon vaatimiin muutoksiin, joita aiheutuu ensisijaisesti joukkojen ja toimijoiden liikkeestä ja tilannetietoisuuden muodostamisesta taistelukentällä. Kognitiivisen verkon avulla voidaan pienentää manuaalisesta verkon suunnittelusta ja konfiguroinnista aiheutuvaa viivettä. Nopeampi verkon konvergoituminen nopeuttaa yhteyden muodostumista ja edelleen tiedon jakamista joukkojen ja toimijoiden välillä. Tietoturva on suuri haaste heterogeenisessa tietoliikenneinfrastruktuurissa ja se on usein hidastava tekijä verkkojen integroinnissa. Kognitiivinen verkko huomioi tietoturvan koko verkon laajuisesti tietoturvakäytännön mukaisesti. Verkko-operaattorista johtuvat inhimilliset virheet ja huolimattomuudet poistuvat. Radiojärjestelmissä kognitiivinen tietoturvatoiminnallisuus mahdollistaa muun muassa elektronisen sodankäynnin huomioimisen.

Verkon resurssien (taajuudet, kapasiteetti, siirtotiet jne) käytössä kognitiivinen verkko on tehokas. Tilannetietoisuus mahdollistaa resurssien järkevän ja taloudellisen käytön siten, että haluttu palvelutaso saavutetaan. Verkko valitsee automaattisesti käytettävät siirtotiet, taajuudet, tietoturvaparametrit ja muut ominaisuudet optimaalisen resurssien käytön saavuttamiseksi. Kognitiivinen verkko parantaa myös yhteentoimivuutta. Verkkojen ja solmujen rajapinnoissa verkot kommunikoivat toistensa kanssa ja tekevät päätöksen käytettävistä protokollista ja parametrien arvoista. Radioverkoissa yhteentoimivuus paranee, kun solmut pystyvät käyttämään joustavasti erilaisia aaltomuotoja. Kognitiivinen verkko mahdollistaa läpinäkyvän kommunikoinnin verkon solmujen kesken.

Mukautumisviiveen vertailu osoittaa, että manuaalisessa järjestelmässä solmujen määrän lisääminen kasvattaa mukautumisviivettä eksponentiaalisesti, kun taas kognitiivisessa järjes-

telmässä se voi olla lähellä lineaarista. Spektrinkäytön tehokkuudessa kognitiivinen verkko on luonnollisesti huomattavasti tehokkaampi, koska se pystyy havainnoimaan spektriä reaaliaikaisesti ja hyödyntämään vapaat taajuudet tehokkaasti. Tehokkuutta lisää erilaisten modulaatio- ja koodausmenetelmien joustava käyttö, jolloin kanavan kapasiteetti saadaan maksimoitua. Kapasiteettia ja samalla elektronista sodankäynnin kykyä parantaa älykkäiden antennien käyttömahdollisuus. Kognitiivinen verkko voi mukauttaa antennien suuntakuviot optimaalisesti tilanteiden ja vaatimusten mukaan. Kognitiivinen verkko parantaa solmujen saavutettavuutta ja sitä kautta järjestelmien yhteentoimivuutta. Nykyjärjestelmissä tietoliikenneyhteys solmusta toiseen sisältää usein erilaisten, jopa manuaalisia rajapintoja ja yhdyskäytäviä, joissa informaation laatu voi huonontua.

Analyysin tulokset osoittavat karkeasti, että kognitiivinen toiminnallisuus mahdollistaa tehokkaamman ja turvallisen tietoliikennejärjestelmän. Vaikka tulokset ovat vain suuntaa antavia, ne osoittavat, että toimiva kognitiivinen järjestelmä pystyy täyttämään verkostopuolustuksen asettamat vaatimukset. Tarkasteltujen ominaisuuksien hyödyntäminen sellaisenaan jatkotutkimuksessa ei välttämättä ole relevanttia, koska vertailun sijaan voi olla mielekkäämpää keskittyä kognitiivisen prosessin tutkimiseen.

Keskeisiä jatkotutkimusalueita ovat verkon tilannetietoisuuden muodostaminen ja päätöksentekoprosessi, tietoturva, palvelutason laatu sekä kognitiivisen kerroksen implementointi tietoliikennejärjestelmiin. Tilannekuvan muodostamisen tutkimuskohteista taktisen verkon kannalta merkittävin on tilannekuvan hajauttaminen tietoturvallisesti siten, että solmuilla on riittävä informaatio tehdä koko verkon kannalta optimaalisia päätöksiä. Päätöksentekomenetelmien tutkimisen tavoitteena on löytää tehokkaat algoritmit monimutkaisten yhtälöiden ratkaisemiseen esimerkiksi antennien suuntakuvioiden määräämiseksi.

Tietoturva on myös tärkeä jatkotutkimusalue. Verkon tekemä väärä päätös voi osoittautua tietoturvan kannalta kriittiseksi. Merkittävä riski taistelukentällä on se, että kriittistä tietoa sisältävä tietoliikenneverkon solmu joutuu vihollisen haltuun. Implementointi tulee jatkumaan haasteellisena laitteiden laskentatehon, koon ja virrankulutuksen vaatimusten suhteen. Palvelutason laatu voi muodostua ongelmaksi kognitiivisissa verkoissa, jos verkon resurssien jakaminen ei ole hallittua. Kognitiivisen kerroksen implementointi tietoliikennejärjestelmiin vaatii tutkimusta tietoliikennejärjestelmän eri kerrosten välisestä vuorovaikutuksesta ja mekanismeista, joilla taataan kerrosten parametrien arvojen mukautuminen päästä-päähän -tavoitteiden mukaisesti.

LÄHTEET

[1] D. S. Alberts & R. E. Hayes, *Planning, Complex Endeavors*, CCRP publication series, USA, 2007.

[2] D. S. Alberts & R. E. Hayes, *Power to the Edge, Command and Control in the Information Age*, 3rd Printing, CCRP publication series, USA, 2003.

[3] D. S. Alberts & R. E. Hayes, *Understanding Command and Control*, CCRP publication series, USA, 2006.

[4] D. S. Alberts, J. J. Garstka & F. P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd Edition (Revised), CCRP publication series, USA, 2000.

[5] D. S. Alberts, J. J. Garstka, R. E. Hayes & D. A. Signori, *Understanding Information Age Warfare*, CCRP publication series, USA, 2001.

[6] *Antenna Patterns and Their Meaning*, White paper, Cisco Systems, Inc, 2007.

[7] S. Antikainen, *Verkostopuolustus ja taktiset periaatteet: Mikä muuttuu?*, Kylkirauta-lehti 3/2006.

[8] A. W. Batschelet, *Effects-based operations: A new Operational Model?*, Strategy Research Project, U.S. Army War College, April 2002.

[9] J. Boyd, *The Essence of Winning and Losing*, a five slide set, June 1995.

[10] S. Ci and J. Sonnenberg, *A Cognitive Cross-Layer Architecture for Next-Generation Tactical Networks*, In Proceedings of IEEE Military Communications Conference, 2007.

[11] *Commander's Handbook for an Effects-Based Approach to Joint Operations*, Joint Warfighting Center, Joint Concept Development and Experimentation Directorate, U.S. Joint Forces Command, 24 February 2006.

[12] *Copernicus: C4ISR for the 21st Century*, Research Report, US Space and Naval Warfare Systems Command (SPAWAR), 1990.

[13] T. H. Cormen, *Introduction to algorithms*, MIT Press, 2001.

[14] P. Demestichas, G. Dimitrakopoulos and A. Alexiou, *Reconfiguration Techniques to Enhance Efficiency Cognitive Networks*, First European Conference on Antennas and Propagation (EuCAP), 2006.

[15] DoD CIO, *Department of Defense Global Information Grid Architectural Vision*, Version 1.0 June 2007. <cio-nii.defense.gov/docs/GIGArchVision.pdf> (viitattu 3.2.2011)

[16] V. F. Fusco, *Foundations of antenna theory and techniques*, Pearson Education, 2005.

[17] V. K. Garg, *Wireless communications and networking*, Morgan Kaufmann, 2007.

[18] J. Garstka and D. Alberts, *Network Centric Operations Conceptual Framework*, Version 2.0, U.S. Office of Force Transformation and Office of the Assistant Secretary of Defense for Networks and Information Integration, 2004.

[19] A. Goldsmith, *Wireless Communications*, Cambridge University Press, 2005.

[20] D. Gonzales, M. Johnson, J. McEver, D. Leedom, G. Kingston, M. Tseng, *Network-Centric Operations Case Study: The Stryker Brigade Combat Team*, RAND, 2005.

[21] R. Heickerö, *Network Based Defence logic - From an innovation point of view*, 10th International Command and Control Research and Technology Symposium (ICCRTS), 2005.

[22] Y. Huang and K. Boyle, *Antennas: from theory to practice*, John Wiley and Sons, 2008.

[23] M. Katz, *Cognac Project Overview*, Presentation in CWC & VTT GIGA Seminar, 4.12.2008.

[24] *Kenttäohjesääntö Yleinen osa (Puolustusjärjestelmän toiminnan perusteet)*, Pääesikunta, Edita Prima, 2008.

[25] J. Kim and J. Shin, *Dynamic network adaptation framework employing layered relative priority index for adaptive video delivery*, Proceedings of IEEE Pacific Rim conference on multimedia No3, 2002.

[26] I. Korkiamäki, *Puolustusvoimien johtamisjärjestelmäala muutoksessa*, Viestimies-lehti 1/2007.

[27] J. Kosola ja J. Jokinen, *Elektroninen sodankäynti, osa 1 - taistelun viides dimensio*, Maanpuolustuskorkeakoulu, Tekniikan laitos, Julkaisusarja 5, No 2, Edita Prima Oy, 2004.

[28] I. Lindell ja K. Nikoskinen, *Antenniteoria*, 848 Otatieto, 1997.

[29] Q. H. Mahmoud (ed.), *Cognitive Networks: Towards Self-Aware Networks*, John Wiley & Sons, Ltd, 2007.

[30] J. N. Mattis, *USJFCOM Commander's Guidance for Effects-based Operations*, Parameters, Vol. XXXVIII, pp. 18-25, Autumn 2008.

[31] P. Mohapatra and S. Krishnamurthy, *Ad hoc networks: technologies and protocols*, Springer, 2005.

[32] *MOT Kielitoimiston sanakirja 2.0*, Internet-sanakirja, Kotimaisten kielten tutkimuskeskus ja Kielikone Oy (viitattu 4.1.2011).

[33] *Network Centric Warfare: Background and Oversight Issues for Congress*, CRS Report for Congress, USA, June 2, 2004.

[34] *Network topology*, Wikipedia, http://en.wikipedia.org/wiki/Network_topology (viitattu 28.2.2011).

[35] *NNEC Best Practices handbook*, Nato Command and Control Centre of Excellence (C2CoE), version 1.0, 2009.

[36] L. Nuaymi, *WiMAX: technology for broadband wireless access*, John Wiley and Sons, 2007.

[37] W. Perry, J. Gordon IV, M. Boito & G. Kingston, *Network-Based Operations for the Swedish Defence Forces: An Assessment Methodology*, Technical Report, RAND Europe, June 2004.

[38] J. G. Proakis and M. Salehi, *Fundamentals of Communication Systems*, Prentice Hall, 2004.

[39] *Puolustusministeriön tietohallintostrategia*, Puolustusministeriö (www.defmin.fi), Kirjapaino Kieli Oy, 2007.

[40] K. Rajala, P. Kesseli, K. Halonen, M. Huttunen, A. Keskinen R. Kuusisto ja A. Arpiainen, *Näkemyksiä maasodan kuvasta*, Taktiikan laitoksen raportti 1/2007.

[41] C. E. Shannon, *A Mathematical Theory of Communication*, Bell Sys. Tech. Journal, pp. 379–423, 623–656, 1948.

[42] T. Sirèn (toim.), *Verkostoavusteinen puolustus 2030*, Maanpuolustuskorkeakoulu, Edita Prima, Helsinki 2009.

[43] Sotatekninen *arvio ja ennuste 2025 (STAE 2025), osa 2 (Puolustusjärjestelmien kehitys)*, Puolustusvoimien Teknillinen Tutkimuslaitos, Edita Prima Oy, Helsinki 2008.

[44] *Suomen turvallisuus- ja puolustuspolitiikka 2004*, Valtioneuvoston selonteko VNS 6/2004, Valtioneuvoston kanslian julkaisusarja 16/2004.

[45] *Suomen turvallisuus- ja puolustuspolitiikka 2009*, Valtioneuvoston selonteko, Valtioneuvoston kanslian julkaisusarja 11/2009.

[46] R. W. Thomas, *Cognitive Networks*, dissertation, Virginia Polytechnic Institute and State University, June 15, 2007.

[47] R. W. Thomas, L. A. DaSilva and A. B. MacKenzie, *Cognitive Networks*, In Proceedings of First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN), 2005.

[48] R. W. Thomas, L. A. DaSilva, M. V. Marathe and K. N. Wood, *Critical Design Decisions for Cognitive Networks*, In Proceedings of IEEE ICC 2007, pp. 3993-3998, June 2007.

[49] R. W. Thomas, D. H. Friend, L. A. DaSilva and A. B. MacKenzie, *Cognitive Networks: Adaptation and Learning to Achieve End-to-End Performance Objectives*, IEEE Communication Magazine, vol. 44, pp. 51-57, Dec. 2006.

[50] UK MOD, *Network Enabled Capability*, Joint Service Publication 777, Edition 1, 2006.

[51] J. Vankka, *Maavoimien taktisen verkon tekniikat ja standardit*, Viestikoulu, Viestirykmentti, Riihimäki, 2009.

[52] J. Velagic, *Design of Smith-like Predictive Controller with Communication Delay Adaptation*, World Academy of Science, Engineering and Technology, Issue 47, 2008.

[53] A. M. Wyglinski, M. Nekovee & Y. T. Hou, *Cognitive radio communications and networks: principles and practice*, Academic Press, 2010.

[54] Y. Zhao, S. Mao, J. O. Neel and J. H. Reed, *Performance Evaluation of Cognitive Radios: Metrics, Utility Functions, and Methodology*, Proceedings of the IEEE, Vol. 97, No. 4, April 2009.

[55] A. E. Zooghby, *Smart antenna engineering*, Artech House, 2005.

LIITTEET

1. Tutkielmassa käytettyjä käsitteitä

TUTKIELMASSA KÄYTETTYJÄ KÄSITTEITÄ

Antennin suuntakuvio (keila) kuvaa antennin lähetystehon tai kentän suuntajakautumaa (ja samalla sen kykyä vastaanottaa säteilyä eri suunnista).

Data, informaatio, tieto ja *tietämys* määrittelevät tiedon luonteen sisällön tason mukaan. Data on tietoverkossa liikkuva, ykkösistä ja nollista muodostuva koodattu merkkijono, jota ei ole tulkittu. Informaatio on merkkijonon ilmaisema viesti. Esimerkiksi tietoverkoissa lähetetty viestin sisältö on informaatiota eli datajonolla on merkitys. Viestissä välittyvän informaation määrä voi olla vastaanottajalle eri kuin lähettäjälle. Tieto on tulkittua ja sisäistettyä informaatiota. Viestin sisällöstä tulee tietoa vasta, kun viestin sisältö on omaksuttu. Tietämyksessä yhdistyy hiljainen tieto ja opittu tieto. Tietämys on tajunnan rakenteissa. Luetun viestin tieto yhdistyy henkilön aiempiin tietoihin ja kokemuksiin.

Diversiteettivahvistus antennijärjestelmissä tarkoittaa sitä, että yhdestä lähteestä lähetetty signaali vastaanotetaan useissa antenneissa, jonka jälkeen vastaanotettuja signaaleita vertaillaan ja laadultaan paras signaali valitaan, jolloin syntyy vahvistusta verrattuna yhden antennin vastaanottoon.

Elektroninen sodankäynti koostuu niistä sotilaallisista toimista, joissa hyödynnetään sähkömagneettista spektriä tai suunnattu energiaa vihollista vastaan. Elektronisella sodankäynnillä tiedustellaan (elektroninen tiedustelu) ja häiritään (elektroninen vaikuttaminen) kohteen sähkömagneettista säteilyä käyttäviä järjestelmiä ja suojataan omat vastaavat järjestelmät.

Itsesynkronointi on termi, joka kuvaa joukon kykyä toteuttaa tehtävä itseohjautuvasti ilman ylemmän johdon jatkuvaa ohjausta ja käskyttämistä. Itsesynkronoinnin kykyyn vaikuttaa keskeisesti tilannetietoisuus varsinkin muiden joukkojen suhteen.

Kognitiivinen prosessi on tietämiseen liittyvä toiminto, joka liittyy ajatteluun (analysointi), ympäristön havainnointiin (tilannetietoisuus) ja sosiaaliseen asetelmaan (kommunikointi). Kognitiiviseen prosessiin liittyy keskeisesti oppiminen.

Kognitiivinen verkko (Cognitive Network, CN) on uudenlainen tietoliikenneverkko, jossa kognitiivinen prosessi havainnoi, analysoi ja tekee päätöksiä verkon mukauttamiseksi asetettujen vaatimusten saavuttamiseksi. Verkko hyödyntää uusinta teknologiaa eri tutkimusaloilta (esim. kone oppiminen, tietämyksen esittäminen, tietoverkko, verkonhallinta). Kognitiivinen verkko kattaa kaikki OSI-mallin kerrokset.

Konfiguroinnilla tarkoitetaan tietoliikenneverkon toimintaparametrien ja -arvojen asettamista. *Paradigmalla* tarkoitetaan jonkin tieteenalan kulloinkin yleisesti hyväksyttyä oppirakennelmaa, ajattelutapaa ja/tai suuntausta [32]. Paradigma on laajasti käytössä oleva, oikeana pidetty, yleisesti hyväksytty ja auktoriteetin asemassa oleva teoria tai viitekehys ja sen mukainen toimintatapa.

Taktisella tietoliikenteellä tarkoitetaan taktisella tasolla (lähinnä prikaati- ja pataljoonataso) tapahtuvaa tietoliikennettä.

Tietoliikenne on tiedon, nykymuodossaan lähinnä sähköisen tiedon, välittämistä. Tavallisimmin tietoliikenteellä tarkoitetaan äänen, kuvien, videon tai muun datan siirtoa yleensä pakettivälitteisen tietoliikenneverkon kautta. Tietoliikenteen merkitys on koko ajan kasvanut jälkiteollisessa yhteiskunnassa. Nykyisin tiedon jakamiseen ja välittämiseen on useita eri tapoja ja standardeja.

Tietoliikenneverkko on tietoliikennelaitteista ja niiden välisistä tiedonsiirtoyhteyksistä muodostuva verkko, jota käytetään tiedon välittämiseen. Tiedonsiirtoyhteydet jaetaan tyypillisesti langallisiin (kupari- ja valokaapelit) ja langattomiin (radioyhteydet).

Tietoliikenneverkon parametri on tietoliikennelaitteessa oleva jonkin ominaisuuden säädettävä muuttuja. Parametri voi olla esimerkiksi taajuus, kaistanleveys, lähetysteho tai käytettävä reititysprotokolla.

Tietoliikenneverkon resurssi on verkon käytössä oleva rajallinen resurssi (esim. taajuus, kanava, rajapinta, linkki tms.), jonka käyttöä voidaan ohjata ja valvoa.

Verkon suorituskyky kuvaa tietoliikenneverkon kykyä toteuttaa toiminnan vaatimat tietoliikennepalvelut. Suorituskykyä voidaan arvioida suhteessa päästä-päähän tavoitteisiin (end-to-end goals).

Verkostokeskeinen sodankäynti on informaatioylivoiman mahdollistava toimintakonsepti [4], joka luo kasvavaa taisteluvoimaa verkottamalla sensorit, päätöksentekijät ja ampujat, jotta saavutetaan yhteinen tietoisuus, kasvava päätöksenteon nopeus, suurempi toiminnan nopeus, kuolettavuus, eloonjäämistodennäköisyys sekä itsesynkronointi.

Verkostopuolustus on suomalainen termi verkostokeskeiselle sodankäynnille. Verkostopuolustus noudattaa verkostokeskeistä paradigmaa, mutta siinä korostuu ei-tekninen ja kokonaismaanpuolustuksellinen verkottuminen.

Yhteensopivuus tarkoittaa järjestelmien komponenttien vaihtokelpoisuutta ja korvattavuutta yhteensopivalla komponentilla. Yhteensopivuus voidaan nähdä yhteentoimivuuden alakäsitteenä.

Yhteentoimivuus tarkoittaa tietojärjestelmien kykyä vaihtaa tietoja keskenään rutiininomaisesti ja automaattisesti. Tietoliikennejärjestelmissä yhteentoimivuus syntyy mm. yhteisistä tietoliikenneprotokollista, tietoturvaratkaisuista ja aaltomuodoista. Yleensä yhteentoimivuus saavutetaan noudattamalla standardeja.